June 2004

AVIATION SECURITY

Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls

GAO

Accountability * Integrity * Reliability

AVIATION SECURITY

Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls

Why GAO Did This Study

In the 2 years since passage of the Aviation and Transportation Security Act (ATSA), the Transportation Security Administration (TSA) has primarily focused its efforts on improving aviation security through enhanced passenger and baggage screening. The act also contained provisions directing TSA to take actions to improve the security of airport perimeters, access controls, and airport workers. GAO was asked to assess TSA's efforts to: (1) evaluate the security of airport perimeters and the controls that limit access into secured airport areas, (2) help airports implement and enhance perimeter security and access controls by providing them funding and technical guidance, and (3) implement measures to reduce the potential security risks posed by airport workers.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security direct TSA's Administrator to develop and provide Congress with a plan for meeting the requirements of the Aviation and Transportation Security Act and taking other actions to improve airport security.

TSA reviewed a draft of this report and generally agreed with GAO's findings and recommendations. Technical comments were incorporated as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-04-728.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

TSA has begun evaluating the security of airport perimeters and the controls that limit access into secured airport areas. Specifically, TSA is conducting compliance inspections and vulnerability assessments at selected airports. These evaluations—though not complete—have identified perimeter and access control security concerns. While TSA officials acknowledged that conducting these airport security evaluations is essential to identifying additional perimeter and access control security measures and prioritizing their implementation, the agency has not determined how the results will be used to make improvements to the entire commercial airport system.

TSA has helped some airport operators enhance perimeter and access control security by providing funds for security equipment, such as electronic surveillance systems. TSA has also begun efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. However, TSA has not begun to gather data on airport operators' historical funding of security projects and current needs to aid the agency in setting funding priorities. Nor has TSA developed a plan for implementing new technologies or balancing the costs and effectiveness of these technologies with the security needs of individual airport operators and the commercial airport system as a whole.

TSA has taken some steps to reduce the potential security risks posed by airport workers. However, TSA had elected not to fully address all related ATSA requirements. In particular, TSA does not require fingerprint-based criminal history checks and security awareness training for all airport workers, as called for in ATSA. Further, TSA has not required airport vendors to develop security programs, another ATSA requirement. TSA said expanding these efforts would require a time-consuming rulemaking process and impose additional costs on airport operators. Finally, although not required by ATSA, TSA has not developed a plan detailing when and how it intends to address these challenges.

Airport Perimeter Access Gate at a Large Commercial Airport

Source: GAO.

United States General Accounting Office

Contents

Figures

Abbreviations

AIP	Airport Improvement Program
AOA	air operations area
ATSA	Aviation and Transportation Security Act
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FSD	federal security director
NCIC	National Crime Information Center
PARIS	Performance and Results Information System
SIDA	security identification display area
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Credential Program

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

June 4, 2004

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

The Honorable Jim Turner
Ranking Minority Member
Select Committee on Homeland Security
House of Representatives

In November 2001, shortly after the September 11 terrorist attacks,
President Bush signed into law the Aviation and Transportation Security
Act, or ATSA (Pub. L. No. 107-71). The act established the Transportation
Security Administration (TSA), giving it responsibility for securing all
modes of transportation, including aviation. One of TSA's first challenges
imposed by the act was to improve the security of airline passenger and
baggage screening activities, activities for which TSA has direct
responsibility. The agency is also taking action to address provisions of
the act to improve three other areas of aviation security: the security of
airport perimeters (such as airfield fencing and access gates), the
adequacy of controls restricting unauthorized access to secured areas
(such as building entry ways leading to aircraft), and security measures
pertaining to individuals who work at airports. Recent media reports of
security breaches and other illegal activities, such as drug smuggling,
taking place at some airports highlight the importance of strengthening
security in these areas. Taken as a whole, these areas, along with
passenger and baggage screening, comprise key elements of the aviation
security environment at commercial airports, both individually and as a
nationwide system.

You requested that we examine TSA's efforts to strengthen security related
to perimeter and access controls. This report assesses TSA's efforts to
(1) evaluate the security of airport perimeters and the controls that limit
access into secured airport areas, (2) help airports implement and enhance
perimeter security and access controls by providing funding and technical
guidance, and (3) implement measures to reduce the potential security
risk posed by airport workers. Due to TSA's concern that the public
release of some of our detailed findings could compromise aviation
security, we also issued a restricted version of this report.

To perform these assessments, we analyzed TSA data on security evaluations conducted and funds distributed to commercial airports for security improvements. We also reviewed pertinent legislation, regulatory requirements, and policy guidance. To determine to what extent TSA had met requirements, we discussed with our Office of General Counsel specific requirements contained in three sections of the act:

- Section 106 (requirements for evaluating airport access controls, testing and evaluating security technologies, and providing technical and financial support to small and medium-sized airports);

- Section 136 (recommending commercially available measures to prevent access to secure airport areas and developing a deployment strategy for available technology at all large airports); and

- Section 138 (performing background checks for all employees with unescorted access to secured airport areas, among others).

We obtained and analyzed TSA data on security breaches, covert testing, inspections of airport compliance with security regulations, and vulnerability assessments. (TSA's covert testing data and information on the test program are classified and are the subject of a separate classified GAO report.) We discussed the threat scenarios used in TSA vulnerability assessments with TSA officials to identify those related to perimeter and access control security. We obtained and analyzed data from the Federal Aviation Administration (FAA) and TSA on perimeter and access control-related security funds distributed to commercial airport nationwide. We reviewed reports on aviation security issued previously by GAO and the Department of Transportation Inspector General.

In addition, we conducted site visits at 12 commercial airports to observe airport security procedures and discuss issues related to perimeter and access control security with airport operator officials. These were Boston Logan International Airport, Atlanta Hartsfield Jackson International Airport, Ronald Reagan Washington National Airport, Washington Dulles International Airport, Orlando International Airport, Tampa International Airport, Miami International Airport, Los Angeles International Airport, San Francisco International Airport, Middle Georgia Regional Airport, Chattanooga Metropolitan Airport, and Columbus Metropolitan Airport. At 10 of these airports, we analyzed a sample of records to verify that the procedures to reduce the security risk of airport workers were followed. We also discussed security issues with TSA airport and headquarters officials, airport security coordinators at each of the nation's 21 largest

and busiest airports (referred to by TSA as "category X" airports), as well as airport industry representatives. More detailed information on our scope and methodology is contained in appendix I. We conducted our review from June 2003 through March 2004 in accordance with generally accepted government auditing standards.

Results in Brief

TSA has begun evaluating the security of airport perimeters and the controls that limit access into secured airport areas, but has not yet determined how the results of these evaluations could be used to make improvements to the nation's airport system as a whole. Specifically, TSA is conducting regulatory compliance inspections, covert testing of selected security procedures, and vulnerability assessments at selected airports. These evaluations—though not yet completed—have identified perimeter and access control security concerns. For example, TSA identified instances where airport operators failed to comply with existing security requirements, including access control-related regulations. (Our evaluation of TSA's covert testing of airport access controls is classified and is discussed in a separate classified report.) In addition, TSA identified threats to perimeter and access control security at each of the airports where vulnerability assessments were conducted in 2003. In January 2004, TSA temporarily suspended its assessment efforts to conduct higher-priority vulnerability assessments dealing with airport vulnerability to shoulder-fired missiles. TSA plans to begin conducting joint vulnerability assessments with the Federal Bureau of Investigation (FBI) but has not yet determined how it will allocate existing resources between its own independent airport assessments and the new joint assessments, or developed a schedule for conducting future vulnerability assessments. In addition, TSA has not yet determined how to use the results of its inspections in conjunction with its efforts to conduct covert testing and vulnerability assessments to enhance the overall security of the nation's commercial airport system.

TSA has helped some airports enhance perimeter and access control security by providing funds for security equipment, such as electronic surveillance systems. TSA has also begun efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. Responsibility for funding most airport security projects shifted in December 2003 from FAA to TSA. As a result, TSA is developing new policies to determine how to review, approve, and prioritize security project funding. However, TSA has not yet begun to gather data on airport operators' historical funding of security projects and current needs to aid the agency in setting funding priorities. Nor has

TSA developed a plan for implementing new technologies or balancing the costs and effectiveness of these technologies with the security needs of individual airports and the commercial airport system as a whole.

TSA has taken some steps to implement measures to reduce the potential security risk posed by airport workers. However, at the time of our review, TSA had not fully addressed all related requirements in the 2001 Aviation and Transportation Security Act. For example, TSA required fingerprint-based criminal history records checks and security awareness training for most, but not all, airport workers called for in the act. TSA relies on background checks as a method of screening most airport workers in lieu of physical screening, as is conducted for passengers and their baggage. However, TSA has not analyzed the security threat posed by airport workers in terms of the potential costs and security benefits of physically screening all airport workers. Further, TSA has not addressed the act's provision that calls for the agency to require that airport vendors with direct access to the airfield and aircraft develop security programs to address security measures specific to vendor employees. TSA said that expanding requirements for background checks and security awareness training for additional workers and establishing requirements for vendor security programs would be costly to implement and would require time-consuming rule-making efforts to assess potential impacts and obtain and incorporate public comment on any proposed regulations.

This report contains recommendations to the Secretary of the Department of Homeland Security (DHS) to help the department articulate and justify future decisions on how best to proceed with security evaluations, fund and implement security improvements—including new security technologies—and implement additional measures to reduce the potential security risks posed by airport workers. We provided a draft of this report to TSA officials who generally concurred with our findings and recommendations. TSA's written comments are presented in appendix III.

Background

ATSA, signed into law on November 19, 2001,[1] shifted certain responsibilities for aviation security from commercial airport operators and air carriers to the federal government and the newly created Transportation Security Administration. Specifically, ATSA granted TSA direct operational responsibility for the screening of passengers and their

---

[1]ATSA, Pub. L. No. 107-71, 115 Stat. 597 (2001).

baggage, as well as responsibility for overseeing U.S. airport operators' efforts to maintain and improve the security of commercial airport perimeters, access controls, and workers. While airport operators, not TSA, retain direct day-to-day operational responsibility for these areas of security, ATSA's sections 106, 136, and 138 direct TSA to improve the security of airport perimeters and the access controls leading to secured airport areas, as well as measures to reduce the security risks posed by airport workers, as shown in figure 1.

Figure 1: ATSA Requirements Directed to TSA Related to Perimeter, Access Control, and Airport Worker Security

Requirements for evaluating airport access controls

Assess and test for airport compliance with access control requirements on an ongoing basis and report annually on the findings of the assessments; assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found. Sec.106(c)(2).

Requirements for strengthening the security of airport perimeters and access controls

Within 6 months after enactment of the act, recommend to airport operators commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons. This 6-month assessment shall review emerging security technologies and procedures and shall include a 12-month deployment strategy for currently available technology at all category X (i.e., the largest and busiest) airports. Sec.136. [a]

Establish a pilot program in no fewer than 20 airports to test and evaluate technology for providing access control and security protections for closed or secure areas. Sec. 106(d).

Develop a plan to provide technical support and financial assistance to small- and medium-sized airports to enhance security operations and to defray the cost of security. Sec. 106(b).

Requirements for reducing the risks posed by airport workers

Perform background checks for all employees with unescorted access to secured airport areas and individuals who have regularly escorted access to secured airport areas and review available law enforcement databases and records of other governmental and international agencies. Sec. 138.

Require airports and air carriers to develop security awareness training programs for airport employees; ground crews; gate, ticket, curbside agents of the air carriers; and other individuals employed at airports. Sec. 106(e).

Require vendors having direct access to the airfield and aircraft to develop their own security programs. Sec. 106(a).

Require screening/inspection of all persons, vehicles, equipment, goods, and property before entering secured areas of U.S. commercial airports. Sec. 106(a).

Source: TSA and GAO.

[a]Section 136 also requires the Secretary of Transportation to conduct a review of reductions in unauthorized access at the category X airports no later than 18 months after the enactment of ATSA.

On February 17, 2002, TSA assumed responsibility from FAA for certain aspects of security at the nation's commercial airports, including FAA's existing aviation security programs, plans, regulations, orders, and directives.[2] Soon thereafter, on February 22, 2002, the Department of Transportation issued regulations to reflect the change in jurisdiction from FAA to TSA.[3] Also, TSA reissued security directives originally issued by FAA after September 11, 2001, related to perimeter and access control security.

TSA hired 158 federal security directors (FSDs) to oversee the implementation of these requirements at airports nationwide. The FSDs also work with inspection teams from TSA's Aviation Regulatory Inspection Division to conduct compliance inspections. In addition, as part of its oversight role, TSA headquarters staff conducts covert testing[4] and vulnerability assessments to help individual airport operators determine how to improve security and to gather data to support systemwide analysis of security vulnerabilities and weaknesses. Airport operators are responsible for implementing TSA security requirements for airport perimeters, access controls, and airport workers. Each airport's security program, which must be approved by TSA, outlines the security policies, procedures, and systems the airport intends to use in order to comply with TSA security requirements.

There are about 450 commercial airports in the United States.[5] Depending upon the type of aircraft operations, airport operators must establish

---

[2]ATSA created TSA as an agency within the Department of Transportation and referred to the head of the TSA as the Under Secretary of Transportation for Security. Since the transfer of TSA to the newly created DHS pursuant to the Homeland Security Act of 2002, Pub. L. 107-296,116 Stat. 2135, the title of the head of TSA has been administratively changed to Administrator. Within DHS, TSA is a distinct entity under the authority of the Under Secretary for Border and Transportation Security.

[3]TSA regulations governing airport security are codified at Title 49 of the Code of Federal Regulations, Chapter XII.

[4]Covert testing involves TSA agents working undercover to evaluate, among other things, the effectiveness of access control processes and procedures.

[5]According to TSA, the total number of commercial airports regulated for security in the United States varies from about 429 to 456, depending on various factors such as the type and level of commercial operations that an aircraft operator conducts at that particular airport, the time of year or season where a particular airport is located, and the economic stability of that airport's region.

either complete, supporting, or partial security programs.[6] Complete security programs include guidelines for performing background checks on airport workers, providing security training for these workers, and controlling access to secured airport areas, among other things. Federal regulations also require that commercial airports with complete security programs designate areas where specific security practices and measures are in place and provide a diagram of these areas. Figure 2 is a diagram of a typical commercial airport and the security requirements that apply to each airport area.

[6]Supporting and partial security programs contain fewer requirements and typically apply to smaller airports. An aircraft operator may receive permission from TSA to amend its security program, provided that the proposed amendments are consistent with safety and the public interest and provide the requisite level of security. Also, if TSA concludes that the needs of safety and the public interest require an amendment to an aircraft operator's security program, the agency may amend the program on its own initiative.

Figure 2: Diagram of Typical Commercial Airport Areas and a Comparison of Security Requirements That Apply to Each Airport Area

Perimeter of entire airport surrounded by fence.

Secured area/ SIDA[a]

AOA/ SIDA

Taxiing areas and runways

Secured area/ SIDA

Secured area/ SIDA

Sterile area

Screening checkpoint

Baggage loading

Passenger boarding gates

Public area

Check-in

AIRPORT ENTRANCE

Secured area/ SIDA

Specified airport areas requiring ID badges

Pick-up and drop-off areas
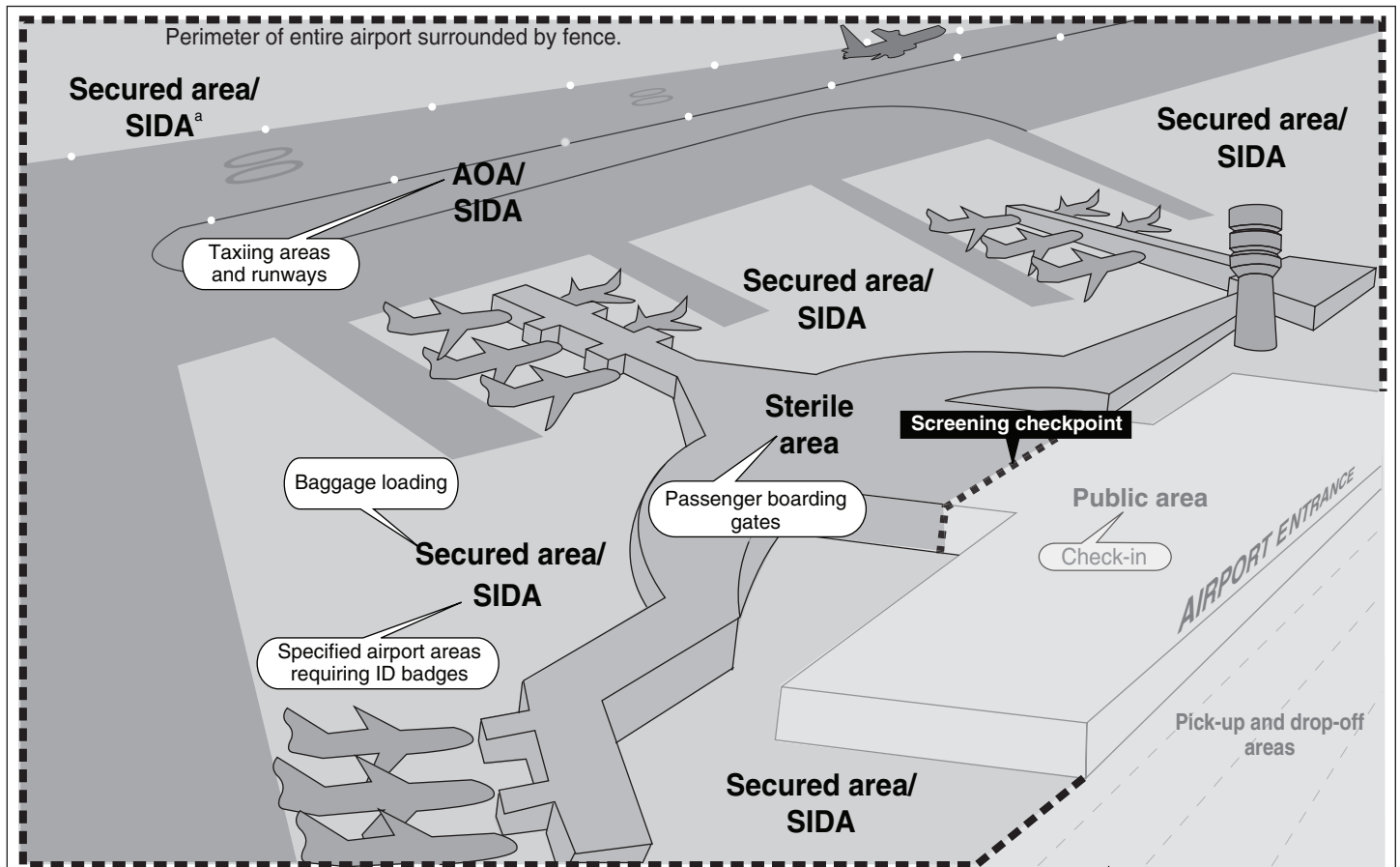
Secured area/ SIDA

[a] Secured/Security Identification Display Area (SIDA)	Air Operations Area (AOA)	Sterile area
• All workers display ID badges • Fingerprint checks for workers prior to being granted unescorted access authority • Workers not required to be physically screened prior to entering these areas • Security awareness training for all workers • Measures to detect and respond to unauthorized presence in this area • Signs at access points and perimeters that warn against unauthorized entry • Access controls used that meet performance standards (e.g. proximity cards and personal identification number)	• If determined by airport to be SIDA, all workers display ID badges • If determined by airport to be SIDA, fingerprints checks for workers prior to being granted unescorted access authority • Workers not required to be physically screened prior to entering these areas • Security awareness training for all workers • Measures to detect and prevent unauthorized presence in this area. • Signs at access points and perimeters that warrant against unauthorized entry	• All workers display ID badges • Fingerprint checks for workers prior to being granted unescorted access authority • Workers are required to be physically screened prior to entering this area, however alternative approaches may be used

Source: GAO.

TSA classifies airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the total number of take-offs and landings annually, the extent to which passengers are screened at the airport, and other special security considerations. U.S. commercial airports are divided into different areas with varying levels of security. Individual airport operators determine the boundaries for each of these areas on a case-by-case basis, depending on the physical layout of the airport. As a result, some of these areas may overlap. Secured areas, security identification display areas (SIDA), and air operations areas (AOA) are not to be accessed by passengers, and typically encompass areas near terminal buildings, baggage loading areas, and other areas that are close to parked aircraft and airport facilities, including air traffic control towers and runways used for landing, taking off, or surface maneuvering. On the other hand, sterile areas are located within the terminal where passengers wait after screening to board departing aircraft. Access to these areas is controlled by TSA screeners at checkpoints where they conduct physical screening of passengers and their carry-on baggage for weapons and explosives.

According to TSA estimates, there are about 1,000,000 airport and vendor employees who work at the nation's commercial airports. About 900,000 of these workers perform duties in the secured or SIDA areas. Airport operators issue SIDA badges to these airport workers. These badges identify the workers and grant them the authority to access the SIDA and secured areas without an escort. Examples of workers with unescorted access to the SIDA and secured areas include workers who access aircraft, including mechanics, catering employees, refuelers, cleaning crews, baggage handlers, and cargo loaders. TSA estimates there are an additional 100,000 employees who work in sterile airport areas, such as the concourse or gate area where passenger flights load and unload. Examples of employees who work or perform duties in the sterile area include those operating concessions and shops, and other air carrier or vendor employees. Other workers may, from time to time, need to enter the SIDA or secured area and must be accompanied by an escort who has been granted unescorted access authority. According to TSA, only a relatively small number of airport workers need regular escorted access to the SIDA and secured areas.[7] Job functions in this category would include delivery personnel, construction workers, and specialized maintenance crews.

---

[7]Regular escorted access is not defined in statute or by regulation.

Methods used by airports to control access through perimeters or into secured areas vary because of differences in the design and layout of individual airports, but all access controls must meet minimum performance standards in accordance with TSA requirements. There are a variety of commercially available technologies that are currently used for these purposes or are used for other industries but could be applied to airports. In addition, TSA has a research and development program to develop new and emerging technologies for these and other security-related purposes.

TSA Has Begun Evaluating Commercial Airport Security but Needs a Better Approach for Assessing Results

TSA has three efforts under way to evaluate the security of commercial airports' perimeters and the controls that limit unauthorized access into secured areas. While ATSA only requires that TSA perform compliance inspections, the agency also relies on covert testing[8] of selected security procedures and vulnerability assessments to meet the legislation's mandate to strengthen perimeter and access control security. TSA acknowledged the importance of conducting these evaluation efforts as an essential step to determine the need for, and prioritization of, additional perimeter security and access control security measures. But the agency has not yet established several elements needed for effective short- and long-term management of these evaluations, such as schedules for conducting its efforts and an analytical approach to using the results of its evaluations to make systematic improvements to the nation's commercial airport system.

TSA Has Revised Its Approach to Conducting Airport Compliance Inspections but Has Not Determined How to Use Results to Strengthen Security

ATSA, (Sec. 106 (c)(2)), requires TSA to assess and test for airport compliance with federal access control security requirements and report annually on its findings. TSA originally planned to conduct comprehensive assessments at each commercial airport periodically. Staff from TSA's Aviation Regulatory Inspection Division along with local airport inspection staff working under federal security directors completed relatively few comprehensive airport inspections in fiscal year 2002, although TSA completed considerably more in 2003. In addition, TSA records indicated that a significant number of individual, or "supplemental" inspections of specific areas of security or local airport security concerns were conducted in fiscal years 2002 and 2003, respectively. TSA, however, did

---

[8]Our evaluation of TSA's covert testing of airport access controls is classified and is discussed in a separate report.

not identify the scope of these inspections, or how many airports were inspected through its supplemental inspections. In addition, the agency did not report on the results of these comprehensive or individual supplemental inspections, as required by ATSA. According to TSA, the agency was limited in its ability to analyze these data because compliance reports submitted during this time frame were compiled in a prototype reporting system that was under development. In July 2003, TSA deployed the automated system—Performance and Results Information System (PARIS)—and began to compile the results of compliance reviews.

In TSA's Annual Inspection and Assessment Plan for fiscal year 2004, TSA revised its approach for reviewing airport operator compliance with security regulations.[9] According to TSA, the new inspection process uses risk management principles that consider threat factors, local security issues, and input from airport operators and law enforcement to target key vulnerabilities and critical assets. Under the new inspection process, the local federal security director at each airport is responsible for determining the scope and emphasis of the inspections, as well as managing local TSA inspection staff. According to the agency, the continuous inspections approach resulted in completion of a significant number of individual inspections of airport access controls and other security requirements in the first few months of fiscal year 2004.

The percentage of inspections that found airport operators to be in compliance with security requirements, including those related to perimeters and access control, was high. According to TSA, its goal is for airport operators to be in 100 percent compliance with security requirements. Despite the generally high compliance rates, TSA identified some instances of airport noncompliance involving access controls.

According to TSA, the agency's new approach to conducting compliance inspections is designed to be a cooperative process based on the premise that voluntary and collaborative airport operator compliance to facilitate solutions to security issues is more effective than the use of penalties to enforce compliance. This approach is intended to identify the root causes of security problems, develop solutions cooperatively with airport operators, and focus the use of civil enforcement actions on the most serious security risks revealed by TSA's inspections. As a result, TSA said that the majority of airport inspection violations related to airport security

---

[9]TSA's inspections review for compliance in 14 areas.

was addressed through on-site counseling with airport operator officials, rather than administrative actions or civil monetary penalties, which TSA is authorized to issue when airport operators fail to address identified areas of noncompliance.[10] According to TSA, on-site counseling is used only for minor infractions that can be easily and quickly corrected. Administrative actions progress from a warning notice suggesting corrective steps to a letter of correction that requires an airport operator to take immediate action to avoid civil penalties. TSA was able to provide the number of cases in which it recommended the issuance of civil penalties to airport operators for violations of security requirement.[11] Table 1 shows the various types of enforcement actions used by TSA to address airport operator noncompliance with security requirements for the period between October 2003 and February 2004.

Table 1: Types of Enforcement Actions Used by TSA to Address Airport Operator Noncompliance with Security Requirements between October 2003 and February 2004

Enforcement action	Sanction used	Number of enforcement actions
Resolved with counseling	None	571
Administrative action	Warning notice	106
	Letter of correction	123
Civil penalties recommended	Monetary	67
Total		**867**

Source: GAO analysis of TSA data.

TSA had not assessed the effectiveness of these penalties in ensuring airport compliance with security requirements as required by ATSA (Sec. 106 (c)(2)). TSA said the agency was not able to conduct inspections at all commercial airports in prior years, or assess the effectiveness of the use of

---

[10]The statutory authority for TSA to issue fines and penalties to individual airport operators, air carriers, and individual airport or airline workers for not complying with established security procedures is 49 U.S.C. § 46301. The penalty for an aviation security violation is found at 49 U.S.C. § 46301(a)(4) and states that the maximum civil penalty for violating chapter 449 [49 U.S.C. §§ 44901 et seq.] or another requirement under this title administered by the TSA's administrator shall be $10,000 except that the maximum civil penalty shall be $25,000 in the case of a person operating an aircraft for the transportation of passengers or property for compensation.

[11]According to TSA, the agency's new automated reporting system documents the number of cases in which a civil penalty was recommended. TSA did not confirm the number of penalties issued.

penalties to ensure airport compliance because of limited personnel assigned to perform these tasks and agency decisions to direct these resources to address other areas of aviation security, such as passenger and baggage screening operations. According to TSA, the primary focus of field inspectors was to monitor passenger and baggage screening operations immediately following the attacks of September 11. As a result, routine inspections were not assigned as high a priority during the months following the attacks. For example, while DHS authorized TSA to use 639 full-time employees for the purpose of performing airport security inspections in fiscal year 2003, TSA allocated 358 full-time employees for this purpose. TSA said that the agency is hiring new regulatory inspectors at airports to help conduct required inspections. In its fiscal year 2005 budget submission, TSA requested over 1,200 full-time employees to conduct compliance inspections.

TSA said airport compliance inspections are needed to ensure that airport operators take steps to address deficiencies as they are identified. TSA also said that the agency has proposed measuring the performance of individual airport against national performance averages, and airports that fall below accepted levels of compliance will receive additional inspections or other actions. However, TSA has not yet developed a plan outlining how the results of its compliance inspections will be used to interpret and help analyze the results of airport vulnerability assessments and covert testing. For example, at the time of our review, a majority of airports tested had high compliance rates, indicating that these airports are implementing most security regulations. However, assessing airport operator compliance with security requirements as a stand-alone measure does not provide a complete picture of the level of security at these airports. Covert testing and vulnerability assessments provide additional information that, taken together with the results of compliance inspections, provide a more complete picture of the security environment at commercial airports on a systemwide basis.

Initial Airport Vulnerability Assessments Reveal Security Concerns, but TSA Lacks Both a Timetable for Completion and a Plan for Making Systematic Improvements

From September to December 2003,[12] TSA conducted vulnerability assessments at some of the nation's commercial airports to help individual airport operators determine how to improve security. At the time of our review, TSA had not established a schedule for completing assessments at the remaining airports. TSA is conducting these vulnerability assessments as part of a broader effort to implement a risk management approach to better prepare for and withstand terrorist threats. A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions. (See app. II for a description of risk management principles and TSA's tools for implementing these principles.)[13] TSA uses various threat scenarios that describe potentially dangerous situations as a basis for conducting its vulnerabilities assessments. During the assessments, TSA and airport operators review the scenarios and rank them according to the risk each poses to the individual airport.

As part of each vulnerability assessment, TSA provided airport operators with a report on the results and recommended short- and long-term countermeasures to reduce the threats identified. According to TSA, some of these countermeasures may be difficult for (1) airport operators to implement because of limited availability of security funding and (2) TSA to mandate because issuing new security regulations is an often time-consuming process that involves public comment and analysis of potential impacts.[14] However, TSA does have authority under 49 U.S.C. § 114(l)(2) to issue regulations or security directives immediately in order to protect transportation security.

Various sources have highlighted the importance of TSA's continuing efforts to assess airport vulnerabilities. For example, in December 2003,

---

[12]Prior to September 2003, TSA completed a vulnerability assessment of a "generic" large airport that focused on threats coming through an airport's perimeter. According to TSA, the assessment and its results, which were issued in October 2002, were of limited value because they focused on one airport area (perimeters) in isolation, and thus needed to be revalidated and updated in the context of the entire airport operation environment.

[13]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001).

[14]We have previously reported on the challenges associated with the issuance of aviation regulations, see U.S. General Accounting Office, *Aviation Rulemaking: Further Reform Is Needed to Address Long-standing Problems*, GAO-01-821 (Washington, D.C.: July 6, 2001).

the President issued a directive[15] calling for assessments of the vulnerability of critical infrastructure, including airports, to assist in developing the nation's homeland security strategy. In addition, TSA data on reported security breaches[16] of airport access controls revealed that such known breaches have increased in recent years.[17] Further, airport operator officials we spoke with noted the importance of vulnerability assessments as the key step in determining needed security enhancements at each airport. Specifically, airport security coordinators at 12 of the nation's 21 largest and busiest airports said that a TSA vulnerability assessment would facilitate their efforts to comprehensively identify and effectively address perimeter and access control security weaknesses.

At the time of our review, TSA had allocated 9 staff to conduct the vulnerability assessments and another 5 staff to analyze the results.[18] According to TSA, these staff also perform other assessment and analytical tasks. Although TSA initially said that it expected to conduct additional assessments in 2004, the agency suspended its efforts to use established threat scenarios to assess vulnerabilities in January 2004. TSA said that the agency elected to redirect staff resources to conduct higher priority assessments of the threat posed by shoulder-fired missiles, also referred to as man portable air defense systems (MANPADS). In addition, TSA said that the agency planned to begin conducting joint vulnerability assessments with the FBI. The FBI previously conducted joint assessments with FAA in response to requirements established in the Federal Aviation Administration Reauthorization Act of 1996. At the time

---

[15]On December 17, 2003, President Bush issued a Homeland Security Presidential Directive (#7) addressing critical infrastructure identification, prioritization, and protection. The directive calls for federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. The directive also requires federal departments and agencies to work with state and local governments and the private sector to accomplish this objective.

[16]A breach of security does not necessarily mean that a threat was imminent or successful. According to TSA, the significance of a breach must be considered in light of several factors, including the intent of the perpetrator and whether existing security measures and procedures successfully responded to, and mitigated against, the breach so that no harm to persons, facilities, or other assets resulted.

[17]According to TSA, differences in the way FAA reported and complied breach data may account for some portion of the increase from 2001 to 2003. Through its PARIS, TSA hopes to standardize breach data reporting in the future. PARIS became operational in July 2003.

[18]The Coast Guard, another agency within DHS, elected to hire a contractor to conduct similar assessments of seaports.

of our review, TSA said that the agency had not yet determined how to allocate its resources to conduct vulnerability assessments using established threat scenarios versus initiating joint assessment efforts with the FBI. When TSA resumes its scenario-based assessment efforts, the agency plans to prioritize its efforts by focusing on the most critical airports. (TSA said the agency intends to determine the criticality of commercial airports based on factors such as current threat intelligence, the number of fatalities that could occur during an attack on the airport, and the economic and sociopolitical importance of the facility.)

After TSA resumes its assessment efforts, the agency intends to compile baseline data on security vulnerabilities to enable it to conduct a systematic analysis of airport security vulnerabilities on a nationwide basis. TSA said such an analysis is essential since it will allow the agency to determine minimum standards and the adequacy of security policies and help the agency and airports better direct limited resources. Nonetheless, at the time of our review, TSA had not yet developed a plan that prioritizes its assessment efforts, provides a schedule for completing these assessments, or describes how assessment results will be used to help guide agency decisions on what, if any, security improvements are needed.

TSA Has Begun Efforts but Has Not Fully Developed Plans to Fund Security Enhancements and Assess Security Technologies

Through funding of a limited number of security enhancements, TSA has helped to improve perimeter and access control security at some airports. However, at the time of our review, TSA had not yet developed a plan to prioritize expenditures to ensure that funds provided have the greatest impact in improving the security of the commercial airport system. Concerning evaluations of security technologies, ATSA contained three provisions (Secs. 136, 106(b), and 106(c)) directing TSA to assess security technologies related to perimeter and access control security and develop a plan to provide technical (and funding) assistance to small- and medium-sized airport operators. TSA has not fully addressed these provisions or developed plans for how and when these requirements will be met. Some airport operators are currently testing or implementing security technologies independently, while others are waiting for TSA to complete its own technology assessments and issue guidance.

TSA Assumed Responsibility for Funding Security Improvements but Has Not Yet Set Priorities

In fiscal years 2002 and 2003, TSA worked with FAA to review and approve security-related Airport Improvement Program (AIP) grant applications[19] for perimeter security and access control projects and other security-related projects. As we reported in October 2002,[20] perimeter and access control security measures—fencing, surveillance and fingerprinting equipment, and access control systems—accounted for almost half of fiscal year 2002 AIP funding for security projects, as shown in table 2.

---

[19]Historically, FAA has provided technical support and financial assistance to airports through its AIP grant program, including the acquisition and installation of security equipment, based on formal requests airport operator officials submitted in accordance with 49 U.S.C. §§ 47101 et seq., and the Airport and Airway Improvement Act of 1982, Pub. L. No. 97-248, 96 Stat. 671.

[20]U.S. General Accounting Office, *Airport Finance: Using Airport Grant Funds for Security Projects Has Affected Some Development Projects*, GAO-03-27 (Washington, D.C.: Oct. 15, 2002).

Table 2: Distribution of AIP Grant Funds Awarded for Security Projects by Project Type, Fiscal Year 2002

Dollars in millions

Type of security project	Grant award amount	Percentage of total security funding
Access control	$141.8	25.3%
Perimeter fencing	78.1	13.9%
Surveillance and fingerprinting equipment	51.4	9.2%
Subtotal	**271.3**	**48.4%**
Other security projects funded (primarily terminal modifications)	289.8	51.6%
Total	**$561.1**	**100.0%**

Source: GAO analysis of AIP grant awards.

In fiscal year 2003, FAA provided a total of $491 million for security-related AIP projects, including about $45.6 million for perimeter fencing projects and another $56.9 million for access control security, a total of about 21 percent of security funding. In addition, Congress appropriated a $175 million supplement to the program in January 2002 to reimburse 317 airports for post-September 11 security mandates.[21]

TSA said that FAA's AIP served as its plan to provide the financial assistance to small and medium-sized airports required by Section 106(b) of ATSA. According to TSA, local federal security directors worked with FAA officials to review and approve security-related AIP grant applications submitted by individual airports, evaluating their merits on an airport-by-airport basis based on guidelines developed and provided by TSA. TSA has not, however, developed an approach to prioritize funding for perimeter and access control security projects at small- and medium-sized (or larger) airports. Without a plan to consider airports' security needs systematically, including those of small- and medium-sized airports, TSA could not ensure that the most critical security needs of the commercial airport system were identified and addressed in a priority order. More importantly, because TSA has assumed primary responsibility for funding security-related projects, FAA's AIP cannot continue to serve as TSA's plan for providing financial assistance to small- and medium-sized airports. Without a plan, TSA could be less able to document, measure,

---

[21]Department of Defense Appropriations Act, Pub. L. No. 107-117, 115 Stat. 2230, 2328 (2002).

and improve the effectiveness of the agency's efforts to provide funding support for enhancing perimeter and access control security.

While acknowledging the lack of a specific plan, TSA said the agency had, in conjunction with FAA, deployed and installed explosive detection systems, explosive trace detection and metal detection devices, and other security equipment at many small- and medium-sized airports for use by federal screeners at those airports and that over 300 small- and medium-sized airports had received technical support and equipment of some kind. However, in advising FAA throughout this process, TSA did not compile and analyze historical information on the cost and types of technology used or the specific airports receiving AIP assistance for perimeter and access control-related security enhancement projects (although TSA stated that historical data were available that could be used to conduct such analyses). FAA has historically maintained data on the uses of AIP funding (including the types of projects funded, amounts, and locations) in a commonly used commercial database system (Access). In addition, airport associations, such as the American Association of Airport Executives, also collect and disseminate information on the use of AIP funds for security enhancements.[22] Without analyses of such historical information, TSA's ability to establish a baseline of security funding for current and future planning efforts to enhance perimeter and access controls could be limited.

In addition to consulting with FAA to provide funding for airport security projects through the AIP, TSA recently began providing security funding directly to airport operators. Specifically, in December 2003, TSA awarded approximately $8 million in grants to 8 airports as part of $17 million appropriated by Congress for enhancing the security of airport terminals, including access controls and perimeter security.[23] Table 3 provides a brief

---

[22]We contacted several airport operators to obtain specific examples of how AIP funds were used. For example, one airport operator used about $2.5 million to upgrade perimeter security and access controls by installing an automatic security gate, connecting perimeter gates to security systems, adding new video screens in the airport emergency operations center, adding motion sensors along airport SIDA perimeters to detect unauthorized intrusion into the SIDA area, among other things. Another airport operator used $884,000 for additional law enforcement personnel, airport surveillance, and the revalidation of airport identification badges.

[23]As part of the 2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States, Pub. L. No. 107-206, 116 Stat. 820, 879-80.

description of the perimeter and access control security-related projects at the 8 airports TSA selected for funding.[24]

Table 3: Distribution of Airports Receiving Grants Awarded by TSA for Perimeter and Access Control-Related Security and Projects Funded

Airport	Funding	Purpose of security project
Providence T. F. Green	$2.38 million	Video surveillance system for detecting and tracking unauthorized persons and vehicles that may breach the perimeter of the airport and advanced ground radar-based security display system for detecting persons or vehicles inside the airport perimeter.
Newark International	$1.67 million	Video surveillance system for detecting and tracking persons and vehicles that breach the airport perimeter.
Helena Regional	$1.2 million	Sensors to detect intruders on airport property.
Boston Logan International Airport	$989,879	Automated system to manage security equipment.
Pittsburgh International	$600,453	Video surveillance system to monitor airport exits from controlled terminal areas.
Chicago Midway Airport	$533,016	Physical barrier system that can be deployed so that the evacuation of an entire concourse may be avoided should an incident occur at the checkpoint.
Denver International	$309,033	Video surveillance system to monitor airport exits from controlled terminal areas.
Key West International	$195,400	Video surveillance system for detecting and tracking persons and vehicles on the air operations area.

Source: GAO analysis of TSA data.

The Vision 100—Century of Aviation Reauthorization Act shifted most of the responsibility for airport security project funding from FAA and the AIP to TSA by establishing a new Federal Aviation Security Capital Fund in December 2003.[25] Through the new fund, Congress authorized up to $500 million for airport security for each fiscal year from 2004 through 2007. Of the total, $250 million will be derived from passenger security fees, along with an additional authorization of up to $250 million. Of this amount, half of the money from each funding source is to be allocated pursuant to a formula that considers airport size and security risk.[26] The

---

[24]After we completed our review, TSA announced the award of an additional $8.2 million in grants to 10 airports for perimeter and access control security-related enhancements.

[25]Vision 100—Century of Aviation Reauthorization Act, Pub. L. No. 108-176, § 605, 117 Stat. 2490, 2566-68 (2003).

[26]Forty percent is allocated to large hub airports, 20 percent for medium hub airports, 15 percent for small and nonhub airports, and 25 percent distributed at the Secretary's discretion on the basis of security risks.

other half would be distributed at the Under Secretary's discretion, with priority given to fulfilling intentions to obligate under letters of intent that TSA has issued. TSA said it is working on, but had not yet developed policies and procedures for, first, defining how the agency will fund and prioritize airport security projects under the new program or second, determining how much, if any, of the new funding will be used for perimeter security and access control projects.[27] However, TSA said that the administration requested in its 2005 budget justification that Congress eliminate the allocation formula so that the agency could allocate funds according to a threat-based, risk assessment approach, regardless of the size of the airport.

TSA Lacks a Technology Plan to Guide Future Enhancements to Airport Perimeter Security and Access Controls

TSA has begun efforts to test commercially available and emerging security technologies to enhance perimeter and access control security. However, TSA has not yet fully addressed three ATSA requirements related to testing, assessing, recommending, and deploying airport security technologies and has not taken steps to otherwise compile and communicate the results of airport operators' independent efforts to test and deploy security technologies.[28]

Two ATSA provisions required that TSA assess technologies for enhancing perimeter and access control security. The first provision (Sec. 136) required that TSA (1) recommend commercially available security measures or procedures for preventing access to secured airport areas by unauthorized persons within 6 months of the act's passage and (2) develop a 12-month deployment strategy for commercially available security technology at the largest and busiest airports (category X).[29] TSA has not explicitly addressed the requirements in this provision and did not meet the associated legislative deadlines. For example, TSA has not recommended commercially available technologies to improve surveillance and use of controls at access points by May 2002 or developed a deployment strategy. TSA said the agency failed to meet these deadlines

[27]The fiscal year 2004 Department of Homeland Security Appropriations Act, Pub. L. No. 108-90, 117 Stat.1137, 1141-42, precludes the obligation or expenditure of any funds to carry out provisions o f the Aviation Security Capital Fund.

[28]GAO has a separate, ongoing review of TSA's research and development program.

[29]Section 136 also requires the Secretary of Transportation to conduct a review of reductions in unauthorized access at the category X airports no later than 18 months after the enactment of ATSA.

because resources and management attention were primarily focused on meeting the many deadlines and requirements associated with passenger and baggage screening, tasks for which TSA has direct operational responsibility.

The second technology provision of ATSA (Sec. 106(d)) requires that TSA establish a pilot program to test, assess, and provide information on new and emerging technologies[30] for improving perimeter and access control security at 20 airports. TSA's $20 million Airport Access Control Pilot Program is intended to assist the agency in developing minimum performance standards for airport security systems, assess the suitability of emerging security technologies, and share resulting information with airport operators and other aviation industry stakeholders. In October 2003, TSA selected a systems integrator to oversee the program and coordinate testing; however, the agency has not selected the specific technologies to be evaluated. TSA plans to look at four areas: biometric identification systems, new identification badges, controls to prevent unauthorized persons from piggybacking (following authorized airport workers into secured areas), and intrusion detection systems.[31] TSA said the agency will conduct the technology assessments in two phases and that the second phase is scheduled to be completed by the end of 2005.[32] However, TSA has not developed a plan describing the steps it will take once the program is completed, although TSA said the agency intends to communicate the results of both assessment phases to airport operators. TSA also said the agency will determine how to use results of the technology assessments and if it will issue any new security or performance standards to airports nationwide when both program assessment phases are completed. Without a plan that considers the potential steps the agency may need to take to effectively use the results of the pilot tests—for example, by issuing new standards—TSA's ability to take effective and immediate steps once the program is completed could be limited.

---

[30]TSA defines new and emerging technologies as commercial products that have not been implemented in an airport security application or products that will be produced in 9 months in sufficient quantities for large-scale deployment.

[31]The requirements to assess biometric identification systems and the controls that prevent unauthorized persons from piggybacking are specified in ATSA, Section 136.

[32]After we completed our review, TSA announced the selection of 8 airports to participate in the first phase of the pilot program.

In addition to the pilot program, testing of a national credentialing system for workers in all modes of transportation—the Transportation Workers Identification Credential (TWIC) Program—is another effort that may help TSA address the requirement in Section 136 of ATSA related to testing and recommending commercially available security technologies to enhance perimeter and access control security. According to TSA, the program is intended to establish a uniform identification credential for 6 million workers who require unescorted physical or cyber access to secured areas of transportation facilities. The card is intended to combine standard background checks and new and emerging biometric technology so that a worker can be positively matched to his or her credential. According to TSA, the agency spent $15 million for the program in fiscal year 2003. In April 2003, TSA awarded a contract for $3.8 million to an independent contractor to assist TSA in the technology evaluation phase of the TWIC program and to test and evaluate different types of technologies at multiple facilities across different modes of transportation at pilot sites. Congress directed $50 million for the TWIC program for fiscal year 2004. This program is scheduled for completion in 2008. We have a separate review under way looking at TSA's TWIC pilot testing at maritime ports and expect to report to the Senate Commerce Committee later this year.

Airport operators and aviation industry associations identified a number of operational issues that they said need to be resolved for the TWIC card to be feasible. For example, they said the TWIC card would have to be compatible with the many types of card readers used at airports around the country, or new card readers would have to be installed. At large airports, this could entail replacing hundreds of card readers, and airport representatives have expressed concerns about how this effort would be funded. According to TSA, however, the TWIC card is intended to be compatible with all airports' card readers. Nonetheless, TSA has not yet conducted an analysis of the cost and operational impacts of implementing the program at airports nationwide. TSA said it intends to gather additional information needed to conduct such an analysis at some point in the future.

The third provision of ATSA related to technology (Sec. 106(b)) requires that TSA develop a plan to provide technical (and funding) support to small- and medium-sized airports. TSA had not developed such a plan. As discussed earlier, TSA said that FAA's AIP was the agency's effort to meet this provision. However, this was an FAA plan and did not fully meet the requirement. More importantly, because the amount of money coming from the AIP for security-related projects will be significantly reduced, and thereby TSA's continuing in involvement with FAA in administering the

program, the AIP cannot continue to serve as TSA's plan for providing technical assistance to small- and medium-sized airports. Without a plan, TSA could be less able to document, measure, and improve the effectiveness of the agency's efforts to provide technical support for enhancing perimeter and access control security.

Airport Operators' Response to Lack of TSA Guidance on Security Technology Varies

We contacted airport operator officials responsible for security at the nation's 21 largest and busiest U.S. commercial airports to obtain their views on the need for technical guidance from TSA to enhance the security of perimeters and access controls. Some airport operators said they were waiting for TSA to complete its technology assessments before enhancing perimeter and access control security, while other airport operators were independently testing and deploying security technologies. Officials at these airports said they are waiting for TSA to provide guidance before proceeding with security upgrades. These airport operators also said that security technology is very costly, and they cannot afford to pay for testing technology prior to purchasing and installing such technology at their airports. They said that information or guidance from TSA about what technologies are available or most effective to safeguard airport perimeters would be beneficial. Conversely, officials at other airports also said they were assessing what is needed to improve their perimeter security and access controls by independently testing and installing security technologies. Several of these officials said that the trial-and-error approach to improving security would not be necessary if TSA would act as a clearinghouse for information on the most effective security technologies and how they can be applied. They said that their independent efforts did not always ensure that increasingly limited resources for enhancing security were used in the most effective way.

In addition to contacting the 21 largest and busiest airports, we identified 13 other airports as examples of airports that have tested or implemented technologies for improving airport perimeter and access control security.[33] Figure 3 shows where various perimeter and access control security technologies were being tested at the time of our review or had been implemented at selected commercial airports across the nation.

---

[33]We identified these 13 airports through our site visits to selected airports and through discussions with officials from one of the primary associations representing airport operators, the American Association of Airport Executives.

Figure 3: Perimeter and Access Control Security Technologies Tested or Implemented at Selected Commercial Airports across the Nation
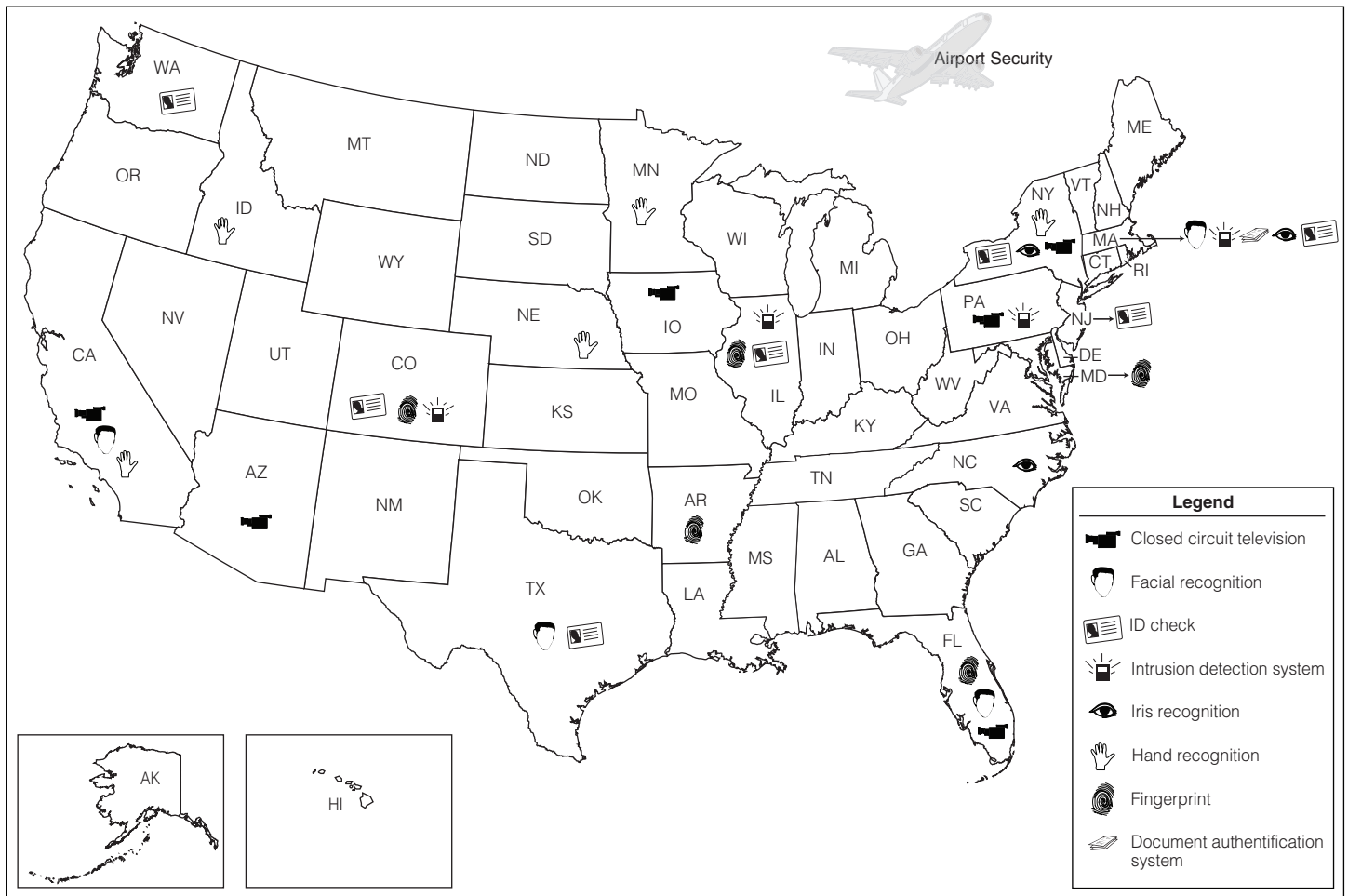
Source: GAO and American Association of Airport Executives.

While some independent efforts have been successful in identifying effective security technologies, others have been less successful. For example, one airport operator said it contracted with a private technology vendor to install identity authentication technology to screen documents presented by job applicants. The airport completed a 5-month pilot program in the fall of 2002 and subsequently purchased two workstations to implement the technology at the airport at a cost of $130,000. Another airport operator conducted an independent pilot program in 2002 to test a biometric recognition system in order to identify airport workers. The system compared 15 airport workers against a database of 250 airport

workers, but operated at a high failure rate. Although compiling information on this pilot test and other airports' efforts would augment TSA's own efforts to assess technology, TSA has not considered the costs and benefits of compiling and assessing the information being collected through these independent efforts. TSA agreed that compiling such data could be beneficial, but the agency had not yet focused its attention on gathering data to generate useful information on such independent testing efforts. Without taking steps to collect and disseminate the results of these independent airport operator efforts to test and deploy security technologies, TSA could miss opportunities to enhance its own testing activities, as well as help other airport operators avoid potentially costly and less effective independent test programs.

TSA Has Helped to Reduce Potential Security Risks Posed by Airport Workers but Has Not Determined How to Fully Address Legislative Requirements

TSA has taken steps to increase measures to reduce the potential security risks posed by airport workers, but it has not addressed all of the requirements in ATSA related to background checks, screening, security training, and vendor security programs or developed plans that describe the actions they intend to take to fully address these requirements. For example, TSA required criminal history records checks and security awareness training for most, but not all, the airport workers called for in ATSA (Secs. 138(a)(8) and 106(e), respectively). Finally, TSA does not require airport vendors with direct access to the airfield and aircraft to develop security programs, which would include security measures for vendor employees and property, as required by ATSA (Sec. 106(a)). TSA cited resource, regulatory, and operational concerns associated with performing checks on additional workers, and providing additional training, as well as the potentially significant costs to vendors to establish and enforce independent security programs. However, TSA had not yet completed analyses to quantify these costs, determine the extent to which the industry would oppose regulatory changes, or determine whether it would be operationally feasible for TSA to monitor implementation of such programs.

Background Checks Are Not Required for All Airport Workers, and the Checks Have Limitations

TSA requires most airport workers who perform duties in secured and sterile areas to undergo a fingerprint-based criminal history records check, and it requires airport operators to compare applicants' names against TSA's aviation security watch lists.[34] Once workers undergo this review, they are granted access to airport areas in which they perform duties. For example, those workers who have been granted unescorted access to secured areas are authorized access to these areas without undergoing physical screening for prohibited items (which passengers undergo prior to boarding a flight). To meet TSA requirements, airport operators transmit applicants' fingerprints to a TSA contractor, who in turn forwards the fingerprints to TSA, who submits them to the FBI to be checked for criminal histories that could disqualify an applicant for airport employment. TSA also requires that airport operators verify that applicants' names do not appear on TSA's "no fly" and "selectee" watch lists to determine whether applicants are eligible for employment.[35]

According to TSA, all airport workers who have unescorted access to secured airport areas—approximately 900,000 individuals nationwide—underwent a fingerprint-based criminal history records check and verification that they did not appear on TSA's watch lists by December 6, 2002, as required by regulation. In late 2002, TSA required airport operators to conduct fingerprint-based checks and watch list verifications for an additional approximately 100,000 airport workers who perform duties in sterile areas. As of April 2004, TSA said that airport operators had completed all of these checks. To verify that required criminal checks were conducted, we randomly sampled airport employee files at 9 airports we visited during our review and examined all airport employee files at a 10th airport.[36] Based on our samples, we estimate that criminal history record checks at 7 of the airports were conducted for 100 percent of the

---

[34]In 49 U.S.C. § 44936 airports and air carriers are required to conduct fingerprint-based criminal history records checks for all workers seeking unescorted access to the SIDA. Specifically, no individual may be given unescorted access authority if he or she has been convicted, or found not guilty by reason of insanity, of any of 28 disqualifying offenses during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

[35]TSA's no-fly list contains the names of individuals that pose, or are suspected of posing, a threat to civil aviation or national security. Individuals on this list will not be permitted to board an aircraft. There is also a selectee process by which individuals who meet certain criteria are set aside for additional screening.

[36]We visited a total of 12 U.S. commercial airports. We did not conduct a records review at the category III and IV commercial airports we visited.

airport employees.[37] In the other 2 airports in which samples were conducted, we estimate that criminal history checks were conducted for 98 percent and 96 percent of the airport workers.[38] At the 10th airport, we examined all airport employee files. We found that criminal history checks were conducted for 93 percent of the airport employees there. Although airport operators could not provide documentation that the checks were conducted in a small number of cases, airport security officials said that no individuals were granted access to secured or sterile areas without the completion of such a check. TSA said that verification of airport compliance with background check requirements was a standard part of airport compliance inspections. For example, according to TSA, the agency conducted criminal history records check verification inspections at 103 airports between October 1, 2003, and February 9, 2004, and found that the airports were in compliance about 99 percent of the time.

TSA does not require airport workers who need access to secured areas from time to time (such as construction workers), and who must be regularly escorted, to undergo a fingerprint check or scan against law enforcement databases, even though such checks are also required by ATSA (Sec. 138(a)(6)). Although TSA does not require that airport operators conduct these checks, TSA drafted a proposed rule in 2002 to require checks on individuals escorted in secured areas. The draft rule also set forth minimum standards for providing escorts for these individuals. In a February 2003 report on TSA's efforts to enhance airport security, the Department of Transportation Inspector General recommended that TSA revise its proposed rule to enhance the security benefits that the new rule could provide by including (1) additional background check requirements, (2) a more specific description of escort procedures, and (3) a clarification on who would be exempt from such requirements.[39] However, at the time of our review, TSA had not addressed these recommendations, issued the proposed rule, or developed a schedule for conducting and completing the rule making process.

---

[37]The 95 percent confidence intervals associated with these estimates extend from 96 percent to 100 percent for 5 of the 7 airports. The analogous interval for a 6th airport extends from 95 percent to 100 percent, and the analogous interval for the 7th airport extends from 94 percent to 100 percent.

[38]The 95 percent confidence intervals for these estimates extend from 92 percent to 99.7 percent, and from 90 percent to 99 percent, respectively.

[39]Department of Transportation Office of Inspector General, *Progress Implementing Sections 106 and 138 of the Aviation and Transportation Security Act*, SC-2003-023, February 27, 2003.

According to TSA, the agency plans to proceed with its rule making to address background checks for those who have regularly escorted access, and, in consultation with DHS and the Office of Management and Budget, has included this rule making as part of a priority list of 20 rule makings that the agency plans to initiate in the next 12 months.

The Effectiveness of Fingerprint-Based Criminal Checks Is Limited

While TSA has taken steps to conduct fingerprint-based checks for airport employees who work in secured and sterile areas, certain factors limit the effectiveness of these checks. For example, fingerprint-based checks only identify individuals with fingerprints and a criminal record on file with the FBI's national fingerprint database. Limitations of these checks were highlighted by recent multifederal agency investigations, which found that thousands of airport workers falsified immigration, Social Security, or criminal history information to gain unescorted access to secured and sterile airport areas.[40] In some of these cases, airport workers who had provided false information to obtain unescorted access underwent a fingerprint-based check and passed.[41] TSA noted that the federal government had not yet developed a system that would allow interagency database searches to provide access to social security and immigration information.[42]

[40]Operation Tarmac was a joint investigation initiated by the Immigration and Naturalization Service, U.S. Attorneys' offices, FBI, Department of Transportation Inspector General, Social Security Administration, and FAA after the September 11 attacks. The operation was aimed at identifying and arresting airport workers who obtained their positions and security status through fraud. Results of the sweeps through airports nationwide has resulted in over 4,200 airport workers being caught having falsified information in order to be hired and be granted SIDA badges. Most of the fraud is through falsification or misrepresentation of Social Security information and immigration documents.

[41]Other airport operator officials we spoke with use additional measures to ensure that an individual provides accurate information prior to being hired at the airport. One airport operator we contacted verifies the accuracy of Social Security numbers and immigration documents before hiring new workers. Officials at this and another airport said they conducted supplemental background checks at the airport operator's own expense to provide further assurance that applicants have no criminal record and have provided accurate information on employment applications. However, these employer checks are not to be confused with, or substitutes for, checks for secured area access badges issued by airport badging authorities.

[42]We previously reported that federal watch lists do not have the capability to automatically share information on immigration status and biographical, financial, and other data. See U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003).

Another limitation with TSA's process for conducting background checks on airport workers is that fingerprint checks do not include a review of, among other things, all available local (county and municipal) criminal record files. As a result, an individual could pass the fingerprint check although he or she had a local criminal record. TSA officials did not consider the lack of a local criminal records check to be a limiting factor because local criminal records are not likely to include any of the 28 criminal convictions that would disqualify an individual from obtaining unescorted access to secured airport areas. According to TSA, local criminal files do not include the more serious crimes such as murder, treason, arson, kidnapping, and espionage that are listed in state and federal criminal databases. Further, several airport operator officials we spoke with expressed concern about cases in which individuals had committed disqualifying criminal offenses and were ultimately granted access to secured areas because federal law (and TSA's implementing regulation) disqualifies an individual only if he or she has been convicted of an offense within 10 years of applying for employment at the airport. Others said that a few disqualifying criminal offenses, such as air piracy, warranted a lifetime rather than a 10-year ban on employment in secured airport areas. Also, current regulation requires that airport workers must report if they are convicted of a crime after the initial criminal check is conducted and surrender their security identification badges within 24 hours of their conviction.[43] In addressing the issue of background checks in May 2003, the Department of Transportation's Inspector General issued a statement supporting random recurrent background checks.[44]

TSA recognizes the potential limitations of current fingerprint check requirements and has taken steps to improve the process. For example, in 2002, TSA began conducting an additional two-part background check consisting of a name-based FBI National Crime Information Center (NCIC) check and a terrorist link analysis against selected terrorism databases for the approximately 100,000 airport workers who perform duties in sterile areas. TSA said it expanded the background check process for these workers because it believed that the cost was more feasible for airport operators to bear, given these workers represent a significantly smaller population than workers who have unescorted access to secured areas.

---

[43]49 C.F.R. § 1542.209(l).

[44]Inspector General, United States Department of Transportation: *Statement Before the National Commission on Terrorist Attacks Upon the U.S. on Aviation Security*, CC-2003-117 (Washington, D.C.: May 22, 2003).

TSA used the NCIC database, a computerized index of documented criminal justice information, to conduct a criminal history record check that compares an individual's name against 19 nationwide criminal history lists.[45] The terrorist link analysis determines whether an airport worker is known to pose a potential terrorist threat. TSA officials noted that the terrorist link analysis could identify personal information on airport employment applications, among other things, thus improving the current background check process.

TSA Faces Challenges in Expanding the Scope of Background Checks

TSA faces challenges in expanding the scope and frequency of current background check requirements to include additional airport workers and more extensive background checks. In terms of expanding background checks to include airport workers who have regularly escorted access to secured areas, TSA said that determining how many workers are regularly escorted in secured airport areas is a challenge because these individuals (such as construction workers) enter the airport on an infrequent and unpredictable basis. TSA said airport officials could not easily determine how many workers are regularly escorted in secured areas and which workers would warrant a background check. TSA had not conducted any sampling or other analysis efforts to attempt to determine how many workers this might include.

In terms of expanding the scope of current background check requirements to include more extensive checks on airport workers who have unescorted access to secured areas, TSA cited the time needed to establish regulatory requirements for the more extensive checks and the potential costs of conducting the checks as challenges. In contrast, to reduce the security risk associated with federal airport screeners, TSA conducts far more extensive checks before providing screeners the same level or lower levels of airport access.

The agency supports conducting the expanded checks for all commercial aviation workers and estimated that the cost to perform fingerprint-based criminal history records checks for all secured and sterile area workers nationwide has been approximately $60 million to $80 million (or about

---

[45]The 19 nationwide criminal files include: stolen article file, boat file, convicted person on supervised release file, convicted sexual offender registry, deported felon file, foreign fugitive file, gun file, license plate file, missing person file, originating agency identifier file, protection order file, securities file, SENTRY file, unidentified persons file, Secret Service Protective order file, vehicle file, violent gang and terrorist organization file, wanted persons file, and vehicle/boat part file.

GAO-04-728 Aviation Security

$60 to $80 for each of the approximately 1 million secured and sterile area workers). TSA had not estimated the costs of applying additional checks to all airport workers. In addition, TSA stated that increasing the frequency of background checks would also increase costs to airport operators. However, TSA had not developed a specific cost analysis to assess the costs of expanding the scope and frequency of the checks or whether the additional security provided by taking such steps would warrant the additional costs.

TSA said the agency is considering alternatives for how these additional checks would be funded. TSA also said that requiring airport workers themselves to pay for a portion of the background check, which is a common practice at some airports, could help to fund these additional checks. In recognition of the potential security risk posed by airport workers, TSA said the agency was weighing the costs and security benefits of expanding the scope and frequency of current background check requirements to include additional airport workers, as well as more extensive checks. However, TSA has not yet established a plan outlining how and when it will do so. For example, TSA has not yet proposed specific analyses to support its decision making or a schedule describing when it plans to decide this issue.

TSA Cites Challenges to Physically Screening All Airport Workers

TSA has different requirements for screening airport workers. For sterile area workers, TSA requires, among other things, that they be screened at the checkpoint. According to TSA's Office of Chief Counsel, TSA intended that sterile area workers be required to enter sterile areas through the passenger-screening checkpoint and be physically screened. However, airport officials, with the FSD's approval, may allow sterile area workers to enter sterile areas through employee access points or may grant them unescorted access authority and SIDA badges.[46]

TSA does not require airport workers who have been granted unescorted SIDA access to be physically screened for prohibited items when entering secured areas. According to TSA, the agency relies on its fingerprint-based criminal history records check as a means of meeting the ATSA

---

[46]The issue of sterile area worker screening was raised at a March 17, 2004, hearing of the Subcommittee on Aviation, House Committee on Transportation and Infrastructure. During the hearing, the chairman asked TSA to survey FSDs to determine how this requirement is being met. In addition, as part of a separate effort, GAO is surveying FSDs, to determine, among other things, the extent to which sterile area workers are being physically screened.

requirement that all individuals entering secured areas at airports be screened and that the screening of airport workers provides at least the same level of protection that results from physical screening of passengers and their baggage. However, as previously noted, there are limitations with the scope and effectiveness of the background check process. TSA acknowledged that physically screening airport workers for access to secured areas could increase security, but it cited challenges such as the need (and associated costs) for more screening staff and increased passenger delays. Although TSA said fingerprint checks are a more economically feasible alternative, the agency had not conducted analyses to determine the actual costs, assessed the potential operational delays that could occur, or the reduction of the risk posed by airport workers that physical screening would provide. However, in October 2002, TSA conducted an analysis of threats posed by airport workers with access to secured areas, and one recommendation in the resulting report was to require airport operators to conduct random physical screening of workers entering secured areas.[47] TSA elected not to adopt this recommendation because of what it characterized as the cost and operational difficulties in physically screening workers. However, TSA did not gather or analyze data from airports to substantiate its claim.

Some airport operator officials we contacted agreed with TSA that physically screening workers prior to entering secured areas would be costly and difficult. For example, some airport operator officials said physical screening of these airport workers would result in increased staffing costs and longer wait times for passengers at passenger-screening checkpoints, or could require screening airport workers at a location separate from passengers to avoid passenger delays. In addition to the operational difficulty of physically screening each worker, TSA and airport operators noted that some airport workers must use prohibited items (such as box cutters and knives) to perform their job functions, and monitoring which workers are allowed to carry such items could be difficult. Also, these prohibited items would still be available to workers who wished to use them to cause harm even after they had been physically screened. At one airport we visited, airport workers who have access to secured areas are required to undergo physical screening when they arrive at work through centralized employee-screening checkpoints but are not

---

[47]U.S. Department of Transportation, Transportation Security Administration, *TSA Airside Security Risk Assessment*, October 3, 2002.

screened when they subsequently enter secured areas through other access points.

TSA has not estimated the cost associated with requiring physical screening of secured area airport workers, although airport operators and industry associations believe the cost would be significant. While TSA is weighing the security benefits of requiring physical screening of workers who have access to secured airport areas against the associated costs, the agency has yet to determine whether such requirements will be established. According to TSA, screening in the form of enhanced background checks on all airport workers—checks that would investigate Social Security information, immigration status, and links to terrorism— would, if instituted, further ensure that airport workers were trustworthy and reduce risk, if not the need to physically screen workers. However, TSA has not developed a plan defining when and how the agency will determine whether it will institute these expanded checks or if physically screening airport workers who need access to secured areas is ultimately necessary and feasible.

TSA Requires Security Training for Some but Not All Airport Workers

ATSA, (Sec. 106(e)), mandates that TSA require airport operators and air carriers to develop security awareness training programs for airport workers such as ground crews, and gate, ticket, and curbside agents of air carriers. However, while TSA requires such training for these airport workers if they have unescorted access to secured areas, the agency does not require training for airport workers who perform duties in sterile airport areas.[48] According to TSA, training requirements for these airport workers have not been established because additional training would result in increased costs for airport operators. Nonetheless, officials at some airports we visited said that the added cost is warranted and have independently required security training for their airport employees that work in sterile areas to increase awareness of their security responsibilities. Among other things, security training teaches airport workers their responsibility to challenge suspicious persons who are not authorized to be in secured areas (an area included in TSA airport covert testing programs). Some airport operator officials said they also used challenge reward programs, whereby airport workers are given rewards

---

[48]TSA regulations governing security training are virtually the same as those required previously under FAA.

for challenging suspicious persons or individuals who are not authorized to be in secured areas, as a way of reinforcing security awareness training.

Many airport operator officials we spoke with were concerned that security training for airport workers in secured areas is not required by TSA regulations on a recurrent basis, an issue previously raised by the Department of Transportation's Inspector General.[49] TSA also agreed that recurrent training could be beneficial in raising the security awareness of airport workers. Although recurrent training is not required by ATSA or by TSA regulation, a federal law does require recurrent security training for the purpose of improving secured area access controls.[50] Other airport operators independently provide recurrent training for individuals who demonstrate a lack of security awareness.

TSA has acknowledged the value of recurrent training for its own workforce. We previously identified that training for TSA employees— airport screeners—should be recurrent, and TSA said it is developing a recurrent training program for its screening workforce to aid in maintaining security awareness, among other things.[51] At the time of our review, TSA said it was considering the benefits of expanding the scope and frequency of security training against the associated costs in time and money to airport operators and businesses. However, TSA had not developed a plan or schedule for conducting the analyses needed to support its decision making or projected when a decision might be made.

---

[49]Inspector General, United States Department of Transportation: *Statement Before the National Commission on Terrorist Attacks Upon the United States on Aviation Security*, CC-2003-117 (Washington, D.C.: May 22, 2003).

[50]See 49 U.S.C. §§ 44903(g)(2)(B), 44935(a),(c).

[51]U.S. General Accounting Office, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173 (Washington, D.C.: Sept. 24, 2003).

TSA Does Not Require Airport Vendors to Develop Their Own Security Programs

TSA has not issued a regulation requiring airport vendors[52] (companies doing business in or with the airport) with direct access to the airfield and aircraft to develop a security program, as required by ATSA (Sec. 106(a)). TSA had not developed an estimate of the number of airport vendors nationwide, although TSA officials said the number could be in the thousands. As an example, security officials at an airport we visited said that over 550 airport vendors conducted business in or with the airport. According to TSA, existing airport security requirements address the potential security risks posed by vendors and their employees. For example, vendor employees that perform duties in secured or sterile areas are required to undergo a fingerprint-based criminal history records check, just as other airport workers are and are prevented by access controls from entering secured airport areas if they are not authorized to do so. However, as discussed above, fingerprint-based criminal history records checks may have limitations.

Many airport operator and airport association officials we spoke with said that requiring vendors to develop their own security program would be redundant because the airport's security program comprises all aspects that a vendor program would include, such as requirements for employee security training, procedures for challenging suspicious persons, background checks, monitoring and controlling employee identification badges, and securing equipment and vehicles. In addition, some said such a requirement would also place a financial and administrative burden on vendors doing business at the airport, particularly the smaller ones, to develop and update such programs. Two airport vendors we spoke with said that developing security programs could be costly, time-consuming, and require the use of a consultant with the necessary security expertise to develop such a plan. In addition, vendors said that airport operators are in the best position and have the necessary expertise to determine security policies for all workers, including vendors, working at the airport.[53]

---

[52]The Department of Transportation's Inspector General recommended that TSA issue this regulation in its Audit Report—Progress Implementing Sections 106 and 138 of the Aviation and Transportation Security Act; Report Number SC-2003-023 (February 27, 2003). Current TSA regulation (1542.113) allows for but does not require airport tenants (entities conducting business on airport property) to develop security programs. TSA did not maintain data on airport vendors or tenants that have developed such a program to date.

[53]According to TSA, current security directives address some aspects of vendor security; however, the specific content of security directives is security sensitive information protected from disclosure under 49 CFR 1520.7(b). As a result, the relevant sections are described in the restricted version of this report.

GAO-04-728 Aviation Security

According to TSA, requiring vendors to develop and maintain their own security programs would also present a resource challenge to TSA's inspection staff. In addition to conducting reviews of airport operator and air carrier compliance with federal security regulations, the already understaffed inspection workforce would also have to determine a way to review vendor security programs and enforce any violations. According to TSA, the process of reviewing the programs and verifying implementation of the program's provisions could require visits to thousands of different vendor locations spread throughout the United States.[54] Despite these challenges, TSA said the agency is considering the costs, benefits, and feasibility of issuing a regulation that would require airport vendors to develop security programs in order to meet the requirements in ATSA. TSA said that it has formed a working group to consider the best approach to take, and this group could become the core of any future rule-making team if necessary. However, the agency has not developed a plan detailing when this analysis will be complete or when any decisions about whether to issue a new rule will be made.

Conclusions

During its first 2 years, TSA assumed a wide variety of responsibilities to ensure that airport perimeter and access controls are secure and that the security risks posed by airport workers are reduced. Given the range of TSA's responsibilities and its relative newness, it is understandable that airport security evaluations remain incomplete and that some provisions of ATSA—which pose operational and funding challenges—have not been met. TSA has begun efforts to evaluate the security environments at airports, fund security projects and test technologies, and reduce the risks posed by airport workers. However, these efforts have been in some cases fragmented rather than cohesive. As a result, TSA has not yet determined how it will address the resource, regulatory, and operational challenges the agency faces in (1) identifying security weaknesses of the commercial airport system as a whole, (2) prioritizing funding to address the most critical needs, or (3) taking additional steps to reduce the risks posed by airport workers. Without a plan to address the steps it will take to fulfill the wide variety of security oversight responsibilities the agency has

---

[54]Depending upon the scope of the possible regulation, the term "vendor" could include all of the companies involved in the supply chain that serves an airport. TSA said that since the supply chain for delivery of office products to the businesses located in the airport's sterile areas could include stages conducted by manufacturers, suppliers, transporters, retailers, and customers, the aggregate number of potential vendors cannot be readily determined.

assumed in the area of perimeter and access control security, TSA will be less able to justify its resource needs and clearly identify its progress in addressing requirements in ATSA and associated improvements in this area of airport security. Such a plan would also provide a better framework for Congress and others interested in holding TSA accountable for the effectiveness of its efforts.

Recommendations for Executive Action

To help ensure that TSA is able to articulate and justify future decisions on how best to proceed with security evaluations, fund and implement security improvements—including new security technologies—and implement additional measures to reduce the potential security risks posed by airport workers, we recommend that the Secretary of Homeland Security direct TSA's Administrator to develop and provide Congress with a plan for meeting the requirements of ATSA. In addition, at a minimum, we recommend the following four actions be addressed:
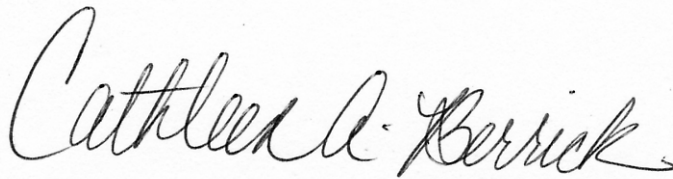
- Establish schedules and an analytical approach for completing compliance inspections and vulnerability assessments for evaluating airport security.

- Conduct assessments of technology, compile the results of these assessments as well as assessments conducted independently by airport operators, and communicate the integrated results of these assessments to airport operators.

- Use the information resulting from the security evaluation and technology assessment efforts cited above as a basis for providing guidance and prioritizing funding to airports for enhancing the security of the commercial airport system as a whole.

- Determine, in conjunction with aviation industry stakeholders, if and when additional security requirements are needed to reduce the risks posed by airport workers and develop related guidance, as needed.

Agency Comments

We provided a draft copy of this report to the Department of Homeland Security and the Transportation Security Administration for their review and comment. TSA generally concurred with the findings and recommendations in the report and provided formal written comments that are presented in appendix III. These comments noted that TSA has started to, or plans to, implement many of the actions we recommended. TSA also provided technical comments that we incorporated as appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this report. At that time, we will send copies to appropriate congressional committees; the Secretary, DHS; the Secretary, DOT; the Director of Office of Management and Budget; and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3404 or at berrickc@gao.gov or Chris Keisling, Assistant Director, at (404) 679-1917 or at keislingc@gao.gov. Key contributors to this report are listed in appendix IV.

Cathleen A. Berrick
Director, Homeland Security
  and Justice Issues

Appendix I: Objectives, Scope, and Methodology

To assess the Transportation Security Administration's (TSA) efforts to (1) evaluate the security of airport perimeters and the controls that limit access into secured airport areas, (2) help airports implement and enhance perimeter security and access controls by providing funding and technical guidance, and (3) implement measures to reduce the potential security risk posed by airport workers, we reviewed pertinent legislation (the Aviation and Transportation Security Act, or ATSA), regulatory requirements, and policy guidance. We discussed specific ATSA requirements related to Sections 106, 136, and 138, which address perimeter and access control security, as well as strengthening requirements for airport workers, with our Office of General Counsel to determine to what extent TSA had met these requirements. We limited our review of TSA's efforts to test, assess, and deploy security technologies as it related to provisions in Sections 106 and 136 of ATSA. We also obtained and analyzed TSA data on security breaches, inspections of airport compliance with security regulations, and vulnerability assessments. (TSA's covert testing data and information on the test program is classified and is the subject of a separate GAO report.) We discussed the threat scenarios used in TSA vulnerability assessments with TSA officials to identify those related to perimeter and access control security. We also obtained and analyzed data from the Federal Aviation Administration (FAA) and TSA on perimeter and access control-related security funds distributed to commercial airports nationwide. We also reviewed reports on aviation security issued previously by us and the Department of Transportation Inspector General.

We discussed the reliability of TSA's airport security breach data for fiscal years 2001, 2002, and 2003 (through October); vulnerability assessment data for 2003; and compliance inspection data for fiscal years 2002, 2003, and 2004 (to February) with TSA officials in charge of both efforts. Specifically, we discussed methods for inputting, compiling, and maintaining the data. In addition, we reviewed reports related to TSA's compliance reviews and vulnerability assessments to determine the results and identify any inconsistencies in the data. Subsequently, no inconsistencies were found, and we determined that the data provided by TSA were sufficiently reliable for the purposes of our review.

In addition, we conducted site visits at 12 commercial airports (8 category X, 1 category I, 1 category II, 1 category III, and 1 category IV) to observe airport security procedures and discuss issues related to perimeter and access control security with airport officials. Airports we visited were Boston Logan International Airport, Atlanta Hartsfield Jackson International Airport, Ronald Reagan Washington National Airport,

Washington Dulles International Airport, Orlando International Airport,
Tampa International Airport, Miami International Airport, Los Angeles
International Airport, San Francisco International Airport, Middle Georgia
Regional Airport, Chattanooga Metropolitan Airport, and Columbus
Metropolitan Airport. We chose these airports on the basis of several
factors, including airport size, geographical dispersion, and airport efforts
to test and implement security technologies. We also conducted
semistructured interviews with airport security coordinators at each of the
21 category X airports to discuss their views on perimeter and access
control security issues. In addition, we contacted or identified 13 other
airports that had tested or implemented perimeter and access control
security technologies.

We reviewed a random sample of 838 airport workers at 10 of the
12 airports we visited (categories X, I, and II) where workers were
indicated as having a fingerprint-based criminal history records check in
calendar year 2003 to verify that these workers had undergone the check.
We did not conduct a records review at the category III and IV commercial
airports we visited. We randomly selected probability samples from the
study populations of airport workers who underwent a fingerprint-based
criminal history record check in the period between January 1, 2003, and
the date in which we selected our sample or December 31, 2003,
whichever was earlier. With these probability samples, each member of
the study populations had a nonzero probability of being included, and
that probability could be computed for any member. Each sample element
selected was subsequently weighted in the analysis to account statistically
for all the members of the population at each airport. Because we followed
a probability procedure based on random selections at each airport, our
samples are only one of a large number of samples that we might have
drawn. Since each sample could have provided different estimates, we
express our confidence in the precision of our particular samples' results
as 95 percent confidence intervals (e.g., plus or minus 7 percentage
points). These are the intervals that would contain the actual population
value for 95 percent of the samples we could have drawn. As a result, we
are 95 percent confident that each of the confidence intervals in this
report will include the true values in the respective study populations.

Further, we interviewed TSA headquarters officials in Arlington, Virginia,
and from the Office of Internal Affairs and Program Review, Office of
Aviation Operations, Office of Chief Counsel, Credentialing Program
Office, Office of Aviation Security Measures, and officials from the Office
of Technology in Atlantic City, New Jersey, to discuss the agency's efforts
to address perimeter and access control security. We also spoke with

officials from two aviation industry associations—the American
Association of Airport Executives and Airports Council International—to
obtain their views on the challenges associated with improving perimeter
and access control security. We also interviewed airport vendors to
determine the need and feasibility of requiring all vendors to develop their
own security programs.

We conducted our work between June 2003 and March 2004 in accordance
with generally accepted government auditing standards.

Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, an individual, or a function and to identify actions to reduce the risk and mitigate the consequences of an attack. Risk management principles acknowledge that while risk cannot be eliminated, enhancing protection from existing or potential threats can help reduce it. Accordingly, a risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions. The purpose of this approach is to link resources with efforts that are of the highest priority. Figure 4 describes the elements of a risk management approach.

Figure 4: Elements of a Risk Management Approach

A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. This assessment represents a systematic approach to identifying potential threats before they materialize, and is based on threat information gathered from both the intelligence and law enforcement communities. However, even if updated often, a threat assessment might not adequately capture some emerging threats. The risk management approach, therefore, uses vulnerability and criticality assessments as additional input to the decision-making process.

A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses. In general, a vulnerability assessment is conducted by a team of experts skilled in such areas as engineering, intelligence, security, information systems, finance, and other disciplines.

A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such, it helps managers to determine operational requirements and target resources at their highest priorities, while reducing the potential for targeting resources at lower priorities.

Source: GAO.

Figure 5 illustrates how the risk management approach can guide decision making and shows that the highest risks and priorities emerge where the three elements of risk management overlap.

**Figure 5: How a Risk Management Approach Can Guide Decision-Making**
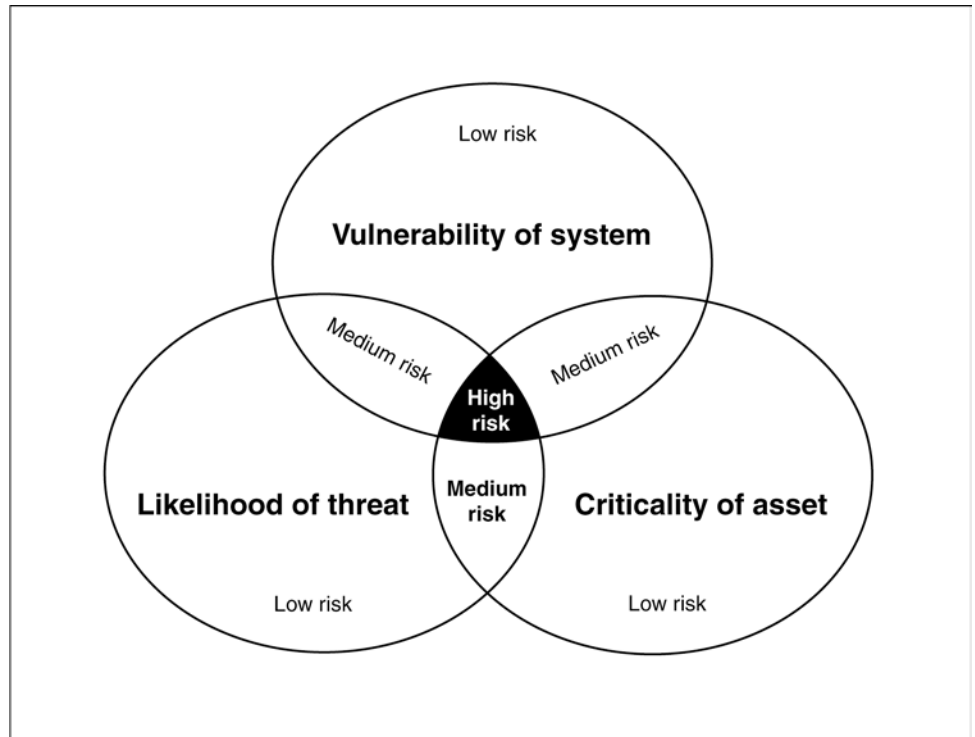
Source: GAO.

For example, an airport that is determined to be a critical asset, vulnerable to attack, and a likely target would be at most risk and, therefore, would be a higher priority for funding compared with an airport that is only vulnerable to attack. In this vein, aviation security measures shown to reduce the risk to the most critical assets would provide the greatest protection for the cost.

According to TSA, once established, risk management principles will drive all decisions—from standard setting to funding priorities and to staffing. TSA has not yet fully implemented its risk management approach, but it has taken steps in this direction. Specifically, TSA's Office of Threat Assessment and Risk Management is in various stages of developing four assessment tools that will help assess threats, criticality, and vulnerabilities. TSA plans to fully implement and automate its risk management approach by September 2004. Figure 6 shows TSA's threat assessment and risk management approach.

Figure 6: TSA's Threat Assessment and Risk Management Approach
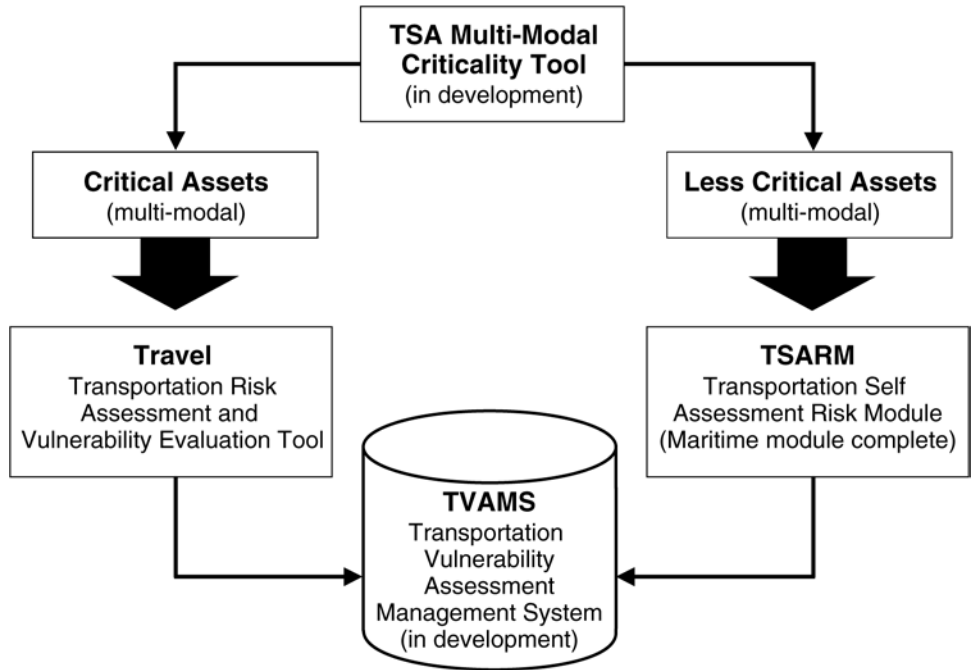
Source: TSA.

The first tool, which will assess criticality, will determine a criticality score for a facility or transportation asset by incorporating factors such as the number of fatalities that could occur during an attack and the economic and sociopolitical importance of the facility or asset. This score will enable TSA, in conjunction with transportation stakeholders, to rank facilities and assets within each mode and thus focus resources on those that are deemed most important. TSA is working with another Department of Homeland Security (DHS) office—the Information and Analysis Protection Directorate—to ensure that the criticality tool will be consistent with DHS's overall approach for managing critical infrastructure.

A second tool—the Transportation Risk Assessment and Vulnerability Tool (TRAVEL)—assesses threats and analyzes vulnerabilities at those transportation assets TSA determines to be nationally critical. The tool is used in a TSA-led and -facilitated assessment that will be conducted on the site of the transportation asset. The facilitated assessments typically take several days to complete and are conducted by TSA subject matter experts, along with airport representatives such as operations

management, regulatory personnel, security personnel, and law enforcement agents. Specifically, the tool assesses an asset's baseline security system and that system's effectiveness in detecting, deterring, and preventing various threat scenarios, and it produces a relative risk score for potential attacks against a transportation asset or facility. Established threat scenarios contained in the TRAVEL tool outlines a potential threat situation including the target, threatening act, aggressor type, tactic/dedication, contraband, contraband host, and aggressor path. In addition, TRAVEL will include a cost-benefit component that compares the cost of implementing a given countermeasure with the reduction in relative risk to that countermeasure. TSA is working with economists to develop the cost-benefit component of this model and with the TSA Intelligence Service to develop relevant threat scenarios for transportation assets and facilities. According to TSA officials, a standard threat and vulnerability assessment tool is needed so that TSA can identify and compare threats and vulnerabilities across transportation modes. If different methodologies are used in assessing the threats and vulnerabilities, comparisons could be problematic. However, a standard assessment tool would ensure consistent methodology.

A third tool—the Transportation Self-Assessment Risk Module (TSARM)—will be used to assess and analyze vulnerabilities for assets that the criticality assessment determines to be less critical. The self-assessment tool included in TSARM will guide a user through a series of security-related questions in order to develop a comprehensive security baseline of a transportation entity and will provide mitigating strategies for use when the threat level increases. For example, as the threat level increases from yellow to orange, as determined by DHS, the assessment tool might advise an entity to take increased security measures, such as erecting barriers and closing selected entrances. TSA had deployed one self-assessment module in support of targeted maritime vessel and facility categories.[1]

The fourth risk management tool that TSA is currently developing is the TSA Vulnerability Assessment Management System (TVAMS). TVAMS is TSA's intended repository of criticality, threat, and vulnerability

---

[1]TSA's Maritime Self-Assessment Risk Module was developed in response to requirements outlined in the Maritime Transportation Security Act of 2002. The act mandates that any facility or vessel that the Secretary believes might be involved in a transportation security incident will be subject to a vulnerability assessment and must submit a security plan to the U.S. Coast Guard.

assessment data. TVAMS will maintain the results of all vulnerability assessments across all modes of transportation. This repository will provide TSA with data analysis and reporting capabilities. TVAMS is currently in the conceptual stage and requirements are still being gathered.

Appendix III: Comments from the Department of Homeland Security

Transportation
Security
Administration

MAY 2 4 2004

Ms. Cathleen Berrick
Director, Homeland Security & Justice Issues
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on GAO's draft report entitled, "Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Control," GAO-04-728.

The Transportation Security Administration (TSA) appreciates the work done in this report to identify areas where security of our Nation's airports may be enhanced. TSA believes that GAO's identification of areas where improvements are needed will contribute to our ongoing efforts to strengthen aviation security. We generally concur with the report and its recommendations and appreciate the discussion of challenges and next steps. However, there are a number of areas within the report about which we would like to comment.

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." The Department of Homeland Security (DHS) is responsible under HSPD-7 for developing a National Critical Infrastructure Protection Plan, which is being managed by the DHS's Information Analysis and Infrastructure Protection Directorate (IAIP). This plan will be comprised of Sector Specific Plans (SSPs), and TSA has been assigned the primary responsibility to coordinate development of the SSP for Transportation. The development of this plan will involve intensive interaction with other DHS directorates and agencies, such as IAIP and the Coast Guard, and the Department of Transportation (DOT) and its modal administrations. The plan, which will be developed over the next several months will identify federal and private-sector stakeholders in each portion of the transportation sector, their roles and relationships; their means of communication; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured and how program effectiveness will be communicated; and how research and development will be prioritized in the sector.

2

The development of the National Critical Infrastructure Protection Plan (NCIPP) and each sector chapter within the NCIPP is a monumental but essential task that requires the support and coordination of Federal departments and agencies, State and local governments, and the private sector.

TSA is on an aggressive timetable to complete the Transportation SSP to feed into the NCIPP. Therefore, while the GAO report concludes that TSA has not yet determined how it "will address the resource, regulatory, and operational challenges the agency faces in identifying security weaknesses of the commercial airport system as a whole," it is TSA's belief that the SSP and the NCIPP will provide the necessary framework and guidance to address challenges and prioritize resources according to the most critical needs across the entire transportation system, including the commercial aviation sector.

Additionally, TSA believes that the report creates the impression that TSA has done less than it actually has to provide security for commercial aviation. Much has been accomplished in the less than two years since enactment of the Aviation and Transportation Security Act (ATSA), and intervening time since completion of the Federalization of passenger security screening at U.S. airports on November 19, 2002. We have instituted a system of reinforcing rings of security to mitigate the risk of future terrorist or criminal acts. These security measures, supported by intelligence and threat analysis, work together to help secure aviation from curbside to cockpit. While no single component of our security system is infallible, we believe our system of mutually supporting rings of security has substantially improved the security of the traveling public. We believe the civil aviation sector is more secure today than it has ever been; however, we are always mindful that there is much yet to be done as we mature our many-layered "system of systems."

While we recognize that the scope of this report was confined to a review of airport perimeter security and access control, it is important to look at the totality of security measures put in place to protect civil aviation in order to completely assess where we are today in regards to aviation security.

3
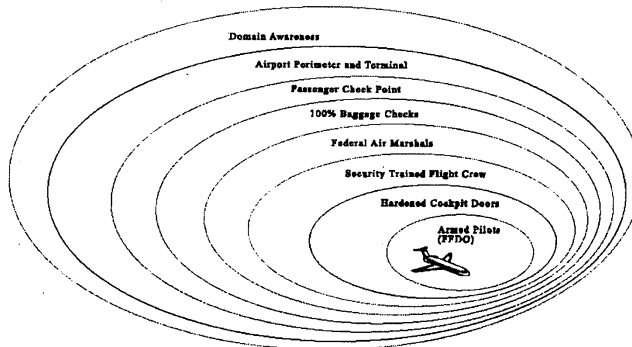
All of the elements in our system of systems complement one another. First, the flow of intelligence information on terrorists, their methods and their plans, has greatly improved our understanding of the threats that we face and helped us to focus our resources on meeting those threats. TSA has also increased the level of existing coordination with our international partners at airports overseas and with air carriers that fly into and out of the United States. TSA and the Federal Aviation Administration (FAA) have helped fund many local airport projects to improve perimeter security, such as the construction of perimeter access roads, the installation of access control systems, electronic surveillance and intrusion detection systems, and security fencing.

Current security directives contain many requirements for implementation by airport and aircraft operators that relate to screening or inspecting people and material entering airport perimeters, including "secured" areas, security identification display areas, and the air operations area where commercial aircraft are located and serviced. For example, these security directives require specific measures at vehicle access gates, inspections of service personnel and their personal property, and identification checks at controlled access points to secured areas. Such countermeasures are implemented systematically at essentially all airports throughout the nation with some variations allowed by request.

TSA works closely with the FAA in the administration of the Airport Improvement Program (AIP), which is an FAA program, to assist in prioritizing applications for security related improvement projects. Federal Security Directors (FSDs) are also involved at the beginning of the AIP application process and actively collaborate with the airport operator to identify projects that would provide the greatest security impact for that particular airport. TSA plans to disseminate guidelines to FSDs to better define and provide guidance on the use of such funds. TSA headquarters personnel and FSDs will use information regarding the way in which these funds are used by the specific airports to make better-informed judgments about proposed security improvements occurring at U.S. airports.

TSA and other DHS component agencies, including Customs and Border Protection and Immigration and Customs Enforcement, continue to work daily with the FAA, DOT and other Federal and State agencies to effectively utilize communal resources to further secure and protect aviation. As we strive for nationwide consistency in the application of reasonable and prudent security measures, we will continue to take local concerns into account. Integrated planning with contributions from industry and local authorities is essential, but we must also maintain the ability to rapidly change security measures based upon the latest assessments from intelligence and law enforcement agencies

Deploying screeners at almost 450 commercial airports around the country less than a year after our establishment was a remarkable feat. Similarly, by December 31, 2002, we met the Congressional deadline in the Aviation and Transportation Security Act to screen checked baggage for explosives. A highly trained force of screeners physically screens every passenger entering the sterile areas of airports. Aviation screeners receive a minimum of 40 hours of classroom training, 60 hours of on-the-job training, and are subject to periodic proficiency assessments and unannounced testing. Screeners are now provided continuous

4

on-the-job training and immediate feedback and remediation through our deployment of the enhanced Threat Image Projection system. They are made aware of new threats and methods of concealment. We have also greatly improved the technology used at screening checkpoints and have improved our capability to detect weapons, explosives, and other prohibited items.

As part of our focus on improved perimeter security, TSA conducts assessments to identify vulnerable areas and needed security measures. The analysis of the results of these assessments will allow TSA to prioritize resources and take necessary steps to close any identified gaps. As you note in your report, TSA redirected resources from assessments using the Transportation Risk Assessment and Vulnerability Evaluation (TRAVEL) tool to conduct MANPADS assessments that were considered a higher priority at the time. Although resources were temporarily redirected from the TRAVEL to MANPADS assessments, a substantial number of compliance inspections were performed during this time, particularly in the areas of access control and access media. TSA's active completion of these MANPADS assessments ultimately provided valuable information for inclusion in broader airport perimeter security assessments at the airports at which they were conducted, helping us to fulfill our compliance inspection plan and develop the self assessment tool for aviation. All this was done in addition to the many layers of security that we have put in place since 9/11. Since the completion of GAO's report, TSA has renewed its TRAVEL efforts, and has begun conducting joint vulnerability assessments (JVA) with the FBI. These vulnerability assessments are threat-based and will be applied at critical commercial airports. The JVA uses current, FBI-developed threat information as its starting point, and then focuses on defining an airport's security system against a current threat. The application of the JVA tool will allow TSA to leverage existing FBI resources and knowledge base to better assess security gaps and vulnerabilities at particular airports. In addition to these government facilitated assessments, a self-assessment tool will be made available to airports that are deemed less critical which focus on prevention and mitigation of a base array of threat scenarios developed for various categories of transportation modes.

As part of our overall strategy to strengthen security of the aviation system, our analysis and evaluation of the results from the security evaluations, various assessments, and compliance inspections will be used to assess priorities and allocate resources to those areas which we believe require additional security measures.

TSA expanded the Federal Air Marshal Service (FAMS) from dozens of agents before 9/11 to thousands of highly trained law enforcement officers, flying the skies on both domestic and international flights. The FAMS transfer to U.S. Immigration and Customs Enforcement (ICE) created a "surge capacity" to effectively support overall homeland security efforts by cross-training FAMs and BICE agents to counter aviation security threats.

Under FAA rules, all commercial passenger aircraft that fly in the United States now have reinforced cockpit doors, making it highly unlikely that terrorists could successfully storm the cockpit. Pilots are now trained to refrain from opening the flight deck door, and if terrorists should somehow breach the reinforced flight deck door, they would meet with a flight deck crew determined to protect the flight deck at all costs. An increasing number of

5

pilots are armed and trained to use lethal force against an intruder on the flight deck. The Federal Flight Deck Officers (FFDOs) that are currently flying have now flown over ten thousand flights, quietly providing another layer of security in our system of systems. As more FFDOs are deputized, this number will rise quickly into the hundreds of thousands of flights. With the enactment of the Vision 100 - Century of Aviation Reauthorization Act (Public Law 108-176), the FFDO program was expanded beyond commercial and charter passenger pilots. Now, cargo pilots and other flightcrew members - specifically flight engineers and navigators on both passenger and cargo planes - are also eligible and being trained for the program.

As you point out in your report, TSA is addressing ATSA requirements related to testing, assessing, and deploying airport security technologies. However, your report states that TSA has not developed a plan to fully address certain sections of ATSA related to perimeter and access control security. Working closely with the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, we have established an ambitious program to develop and deploy new security technologies and use technology to enhance human performance. Our efforts are well underway. TSA is currently involved in several programs that meet the ATSA requirements to assess security technologies and has provided guidance to FSDs and airport operators on security technologies. TSA recently selected eight airports to participate in Phase I of the Access Control Pilot Program, which will test Radio Frequency Identification (RFID) technology, anti-piggybacking technology, advanced video surveillance technology, and various biometric technologies. Testing this off-the-shelf technology will give TSA the ability to determine the suitability of use in a real-world operational environment. Based on this analysis, TSA will then determine which technologies will be evaluated in Phase II. The information gleaned from this pilot will then be provided to industry representatives so that they may make informed decisions when designing access control systems to meet their security and regulatory needs. We also have a robust test and evaluation program that has evaluated a number of biometric devices, perimeter intrusion sensors, and anti-piggybacking devices. Our program also includes developmental efforts such as the ASDE-3/X radar enhancement program to allow this deployed equipment to detect potential perimeter intrusion events. Additionally, TSA has developed a number of guides to assist in selecting and deploying security technologies, including reports with subjects such as perimeter security design, biometrics at domestic airports, and technology to address tailgating and piggybacking

In addition to the Access Control Pilot Program, TSA recently awarded Airport Terminal Security Enhancement grants totaling $8.2 million to ten airports. The grants will be used to deploy various technologies, including state-of-the-art video surveillance and RFID tags to track the location of mobile resources such as baggage carts and other vehicles in the secure areas of the airports. The first round of grants for terminal improvements was awarded in December 2003 to eight airports. This program is part of TSA's ongoing effort to work with the airports and private industry to explore and deploy the most advanced technology commercially available to enhance security for the aviation system.

As you also point out in your report, TSA expanded coverage of the aviation workforce with background checks when we directed that all sterile area workers undergo a two-part

6

check in late 2002 and early 2003. Further, we are planning to conduct enhanced background checks on all sterile area and SIDA workers this year.

In further identifying the challenges that TSA faces in ensuring the effective and efficient security of the aviation system as a whole, TSA looks to partnerships created through stakeholder outreach, which has always been a priority for TSA. We work collaboratively with industry management and labor, and consumer stakeholders in identifying opportunities to increase efficiency and areas for improvement. We will continue to involve stakeholders in our decision-making process and communicate regularly and clearly with our customers, our partners, and our employees. In fact, TSA is actively involved in the development of a process tool to provide information to decision makers to achieve a balance of safety, security, and efficiency. The U.S. Commercial Aviation Partnership (USCAP) is a process that allows stakeholders to define areas of consensus and disagreement on the costs and benefits of significant security proposals. This tool is a means to focus stakeholder discussions on policy and economic impacts. TSA has the opportunity to use this tool as one source for the mandatory regulatory evaluation and to encourage policy discussions with meaningful cost and benefit comparisons.
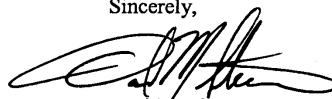
TSA also continues to capitalize on its Federal partnerships and working with the DHS S&T Directorate, TSA is beginning a comprehensive review of the civil aviation security system now that over two years have passed since the enactment of the Aviation and Transportation Security Act and nearly fourteen years have passed since the Aviation Security Improvement Act of 1990. We are incorporating this review as part of our constant evaluation of the security measures we have put into place, and will be able to use the results of this report, along with our other evaluative efforts to consider other approaches to improved aviation security that may be available. We have learned a great deal very quickly, but there is still more to do to successfully accomplish our transportation security mission. Much of this additional work hinges on understanding the bigger picture of our national transportation security system, which is intermodal, interdependent, and international in scope.

In sum, we appreciate your review of perimeter security and access control and commend you for the thorough analysis and discussion that comprises this report. We believe many of your recommendations are already being addressed by efforts well underway. As we continue to be cognizant of the areas where we can improve, we remain vigilant and focused on the security challenges we face.

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

Sincerely,

David M. Stone, ADM
Acting Administrator

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Norman J. Rabkin (202) 512-3610
Cathleen A. Berrick (202) 512-3404
Chris Keisling (404) 679-1917

Staff Acknowledgments

In addition to those named above, Leo Barbour, Amy Bernstein, Christopher Currie, Dave Hooper, Thomas Lombardi, Sara Ann Moessbauer, Jan Montgomery, Steve Morris, Octavia Parks, Dan Rodriguez, and Sidney Schwartz were key contributors to this report.