United States General Accounting Office

GAO

Testimony before the Committee on Commerce, Science and Transportation, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, November 5, 2003

AVIATION SECURITY

Efforts to Measure Effectiveness and Address Challenges

Statement of Cathleen A. Berrick, Director
Homeland Security and Justice Issues

November 5, 2003

AVIATION SECURITY

Efforts to Measure Effectiveness and Address Challenges

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-232T, a testimony to the Committee on Commerce, Science and Technology, U.S. Senate

Why GAO Did This Study

It has been 2 years since the attacks of September 11, 2001, exposed vulnerabilities in the nation's aviation system. Since then, billions of dollars have been spent on a wide range of initiatives designed to enhance the security of commercial aviation. However, vulnerabilities in aviation security continue to exist. As a result, questions have been raised regarding the effectiveness of established initiatives in protecting commercial aircraft from threat objects, and whether additional measures are needed to further enhance security. Accordingly, GAO was asked to describe the Transportation Security Administration's (TSA) efforts to (1) measure the effectiveness of its aviation security initiatives, particularly its passenger screening program; (2) implement a risk management approach to prioritize efforts and focus resources; and (3) address key challenges to further enhance aviation security.

What GAO Recommends

In prior reports and testimonies, GAO has made numerous recommendations to strengthen aviation security and to improve the management of federal aviation security organizations. We also have ongoing reviews assessing many of the issues addressed in this testimony and will issue separate reports on these areas at a later date.

www.gao.gov/cgi-bin/getrpt?-GAO-04-232T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen A. Berrick at (202) 512-8777 or bbeberrickc@gao.gov..

What GAO Found

TSA has implemented numerous initiatives designed to enhance aviation security, but has collected limited information on the effectiveness of these initiatives in protecting commercial aircraft. Our recent work on passenger screening found that little testing or other data exist that measures the performance of screeners in detecting threat objects. However, TSA is taking steps to collect data on the effectiveness of its security initiatives, including developing a 5-year performance plan detailing numerous performance measures, as well as implementing several efforts to collect performance data on the effectiveness of passenger screening—such as fielding the Threat Image Projection System and increasing screener testing.

Passenger Screening Checkpoint at U.S. Airport

Source: FAA.

TSA has developed a risk management approach to prioritize efforts, assess threats, and focus resources related to its aviation security initiatives as we previously recommended, but has not yet fully implemented this approach. 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. TSA is developing and implementing both a criticality and a vulnerability assessment tool to provide a basis for risk-based decision-making. TSA is currently using some components of these tools and plans to fully implement its risk management approach by the summer 2004.

TSA faces a number of programmatic and management challenges as it continues to enhance aviation security. These include the implementation of the new computer-assisted passenger prescreening system, as well as strengthening baggage screening, airport perimeter and access controls, air cargo, and general aviation security. TSA also must manage the costs associated with aviation security and address human capital challenges, such as sizing its workforce as efficiency is improved with security-enhancing technologies—including the integration of explosive detection systems into in-line baggage-handling systems. Further challenges in sizing its workforce may be encountered if airports are granted permission to opt out of using federal screeners.

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to participate in today's hearing to discuss the security of our nation's aviation system. It has been more than 2 years since the attacks of September 11, 2001, exposed vulnerabilities in commercial aviation. Since then, billions of dollars have been spent and a wide range of programs and initiatives have been implemented to enhance aviation security. However, recent reviews and covert testing conducted by GAO and Department of Homeland Security Office of Inspector General, as well as media reports, revealed continuing weaknesses and vulnerabilities in aviation security. For example, the recent incident involving a college student who placed box cutters, clay resembling plastic explosives, and bleach on commercial aircraft illustrated that aviation security can still be compromised. As a result of these challenges, the Transportation Security Administration (TSA), which is responsible for ensuring the security of aviation, is faced with the daunting task of determining how to allocate its limited resources to have the greatest impact in addressing threats and enhancing security.

My testimony today focuses on three areas that are fundamental to TSA's success in allocating its resources and enhancing aviation security. These areas are (1) the need to measure the effectiveness of TSA's aviation security initiatives that have already been implemented, particularly its passenger screening program; (2) the need to implement a risk management approach to prioritize efforts, assess threats, and focus resources; and (3) the need to address key programmatic and management challenges that must be overcome to further enhance aviation security. This testimony is based on our prior work, reviews of TSA documentation, and discussions with TSA officials.

In summary:

Although TSA has implemented numerous programs and initiatives to enhance aviation security, it has collected limited information on the effectiveness of these programs and initiatives. Our recent work on TSA's passenger screening program showed that although TSA has made numerous enhancements in passenger screening, it has collected limited information on how effective these enhancements have been in improving screeners' ability to detect threat objects. The Aviation and Transportation Security Act (ATSA), which was enacted with the primary goal of strengthening the security of the nation's aviation system, requires that TSA establish acceptable levels of performance for aviation security initiatives and develop annual performance plans and reports to measure

and document the effectiveness of those initiatives.[1] Although TSA has developed an annual performance plan and report as required by ATSA, to date these tools have focused on TSA's progress in meeting deadlines to implement programs and initiatives mandated by ATSA, rather than on the effectiveness of these programs and initiatives. TSA has recognized that its data on the effectiveness of its aviation security initiatives are limited and is taking steps to collect objective data to assess its performance, which is to be incorporated in DHS's 5-year performance plan.

TSA has developed a risk management approach to prioritize efforts, assess threats, and focus resources related to its aviation security initiatives as recommended by GAO, but has not yet fully implemented this approach. TSA's aviation security efforts are varied and vast, and its resources are fixed. As a result, a risk management approach is needed to better support key decisions, linking resources with prioritized efforts.[2] TSA has not yet fully implemented its risk management tools because until recently its resources and efforts were largely focused on meeting the aviation security mandates included in ATSA. TSA has acknowledged the need for a risk management approach and expects to complete the development and automation of its risk management tools by September 2004.

TSA faces a number of programmatic and management challenges as it continues to address threats to our nation's aviation system. These challenges include implementing various aviation security programs, such as the Computer-Assisted Passenger Prescreening System[3]—CAPPS II—and addressing broader security concerns related to the security of air cargo and general aviation.[4] TSA also faces challenges in managing the costs of aviation security and in strategically managing its workforce of about 60,000 people, most of whom are deployed at airports to detect weapons and explosives. TSA has been addressing these and other

[1]P.L. 107-71.

[2]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 by linking resources with prioritized efforts.

[3]CAPPS II is a system intended to perform a risk assessment of all airline passengers to identify those requiring additional security attention.

[4]General aviation consists of all civil aircraft and excludes commercial and military aircraft.

challenges through a variety of efforts. We have work in progress that is examining TSA's efforts in addressing many of these challenges.

Background

Ensuring the security of our nation's commercial aviation system has been a long-standing concern. As demonstrated by the 1988 bombing of a U.S. airliner over Lockerbie, Scotland, and the 1995 plot to blow up as many as 12 U.S. aircraft in the Pacific region discovered by Philippine authorities, U.S. aircraft have long been a target for terrorist attacks. Many efforts have been made to improve aviation security, but as we and others have documented in numerous reports and studies, weaknesses in the system continue to exist. It was these weaknesses that terrorist exploited to hijack four commercial aircraft in September 2001, with tragic results.

On November 19, 2001, the President signed into law the Aviation and Transportation Security Act, with the primary goal of strengthening the security of the nation's aviation system. ATSA created TSA as an agency within the Department of Transportation with responsibility for securing all modes of transportation, including aviation. ATSA mandated specific improvements to aviation security and established deadlines for completing many of them. TSA's main focus during its first year of operation was on meeting these ambitious deadlines, particularly federalizing the screener workforce at commercial airports nationwide by November 19, 2002, while at the same time establishing a new federal organization from the ground up. The Homeland Security Act, signed into law on November 25, 2002, transferred TSA from the Department of Transportation to the new Department of Homeland Security.[5]

Virtually all aviation security responsibilities now reside with TSA, including the screening of air passengers and baggage, a function that had previously been the responsibility of air carriers. TSA is also responsible for ensuring the security of air cargo and overseeing security measures at airports to limit access to restricted areas, secure airport perimeters, and conduct background checks for airport personnel with access to secure areas, among other responsibilities.

[5]P.L. No. 107-296.

Limited Information Exists on the Effectiveness of Aviation Security Initiatives

TSA has implemented numerous initiatives designed to enhance aviation security but has collected little information on the effectiveness of these initiatives. ATSA requires that TSA establish acceptable levels of performance and develop annual performance plans and reports to measure and document the effectiveness of its security initiatives.[6] Although TSA has developed these performance tools, as required by ATSA, it currently focuses on progress toward meeting ATSA deadlines, rather than on the effectiveness of its programs and initiatives. However, TSA is taking steps to collect objective data to assess its performance.

Evaluation of Program Effectiveness

TSA currently has limited information on the effectiveness of its aviation security initiatives. As we reported in September 2003,[7] the primary source of information collected on screeners' ability to detect threat objects is the covert testing conducted by TSA's Office of Internal Affairs and Program Review. However, TSA does not consider the results of these covert tests to be a measure of performance but rather a "snapshot" of a screener's ability to detect threat objects at a particular point in time, and as a system-wide performance indicator. At the time we issued our report, the Office of Internal Affairs and Program Review had conducted 733 covert tests of passenger screeners at 92 airports. Therefore, only about 1 percent of TSA's nearly 50,000 screeners had been subject to a covert test.

In addition to conducting covert tests at screening checkpoints, TSA conducts tests to determine whether the current Computer-Assisted Passenger Screening System is working as designed, threat objects are detected during the screening of checked baggage, and access to restricted areas of the airport is limited only to authorized personnel.[8] While the

[6]An annual performance plan is to provide the direct linkage between the strategic goals outlined in the agencies' strategic plan and the day-to-day activities of managers and staff. Additionally, annual performance plans are to include performance goals for an agency's program activities as listed in the budget, a summary of the necessary resources that will be used to measure performance, and a discussion of how the performance information will be verified. An annual performance report is to review and discuss an agency's performance compared with the performance goals it established in its annual performance plan.

[7]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).

[8]The original Computer Assisted Passenger Screening System is a stand-alone application residing in an air carrier's reservation system that analyzes certain behavioral patterns to score and calculate each passenger's need for additional screening.

Office of Internal Affairs has conducted about 2,000 access tests, it has conducted only 168 Computer-Assisted Passenger Screening System and checked baggage tests. Based on an anticipated increase in staff from about 100 in fiscal year 2003 to 200 in fiscal year 2004, the Office of Internal Affairs and Program Review plans to conduct twice as many covert tests next year.[9]

Another key source of data on screener performance in detecting threat objects is the Threat Image Projection (TIP) system, which places images of threat objects on the X-ray screen during actual operations and records whether screeners identify the threat object.[10] The Federal Aviation Administration began deploying TIP in late 1999 to continuously measure screener performance and to train screeners in becoming more adept at detecting hard-to-spot threat objects. However, TIP was shut down immediately following the September 11 terrorist attacks because of concerns that it would result in screening delays and panic, as screeners might think that they were actually viewing a threat object. Although TSA officials recognized that TIP is a key tool in measuring, maintaining, and enhancing screener performance, they only recently began reactivating TIP on wide-scale basis because of competing priorities, a lack of training, and a lack of resources needed to deploy TIP activation teams. Once TIP is fully deployed and operational at every checkpoint at all airports, as it is expected to be in April 2004, TSA headquarters and federal security directors[11] will have the capability to analyze this performance data in a number of ways, including by individual screeners, checkpoints, terminals, and airports.

When fully deployed, the annual screener recertification test results will provide another source of data on screener performance. ATSA requires

[9]Currently, the Office of Internal Affairs and Program Review has 7 team leaders assigned full-time to covert testing and plans to have a total of 14 full-time team leaders by the end of December 2003. The team leaders draw from the remaining staff within the office, such as auditors and analysts, to perform the testing. According to TSA officials, overall, 95 percent of the staff in the Office of Internal Affairs and Program Review participate in covert testing as a collateral responsibility.

[10]TIP is designed to test screeners' detection capabilities by projecting threat images, including guns and explosives, into bags as they are screened. Screeners are responsible for positively identifying the threat image and calling for the bag to be searched. Once prompted, TIP identifies to the screener whether the threat is real and then records the screener's performance in a database that could be analyzed for performance trends.

[11]Federal security directors oversee security at each of the nation's commercial airports.

that TSA collect performance information on each screener through conducting an annual proficiency review to ensure he or she continues to meet all qualifications and standards required to perform the screening function. Although TSA began deploying federal screeners to airports in April 2002, TSA only recently began implementing the annual recertification program and does not expect to complete testing at all airports until March 2004. The recertification testing is comprised of three components: (1) image recognition; (2) knowledge of standard operating procedures; and (3) practical demonstration of skills, to be administered by a contractor. TSA officials consider about 28,000 screeners as having already completed the first two components because they successfully passed competency tests TSA administered at many airports as part of a screener workforce reduction effort. However, these competency tests did not include the third component of TSA's planned annual screener recertification program—the practical demonstration of skills. TSA officials awarded a contract for this component of the annual proficiency reviews in September 2003.

TSA's Performance Management Information System for passenger and baggage screening operations is designed to collect performance data, but it currently contains little information on screener performance in detecting threat objects. The Performance Management Information System collects a wide variety of metrics on workload, staffing, and equipment and is used to identify some performance indicators, such as the level of absenteeism, the average time for equipment repairs, and the status of TSA's efforts to meet goals for 100 percent electronic baggage screening.[12] However, the system does not contain any performance metrics related to the effectiveness of passenger screeners. TSA is planning to integrate performance information from various systems into the Performance Management Information System to assist the agency in making strategic decisions. TSA further plans to continually enhance the system as it learns what data are needed to best manage the agency. In addition to making improvements to the Performance Management Information System, TSA is currently developing performance indexes for both individual screeners and the screening system as a whole. The screener performance index will be based on data such as the results of performance evaluations and recertification tests, and the index for the screening system will be based on information such as covert test results

[12]The Performance Management Information System also contains metrics on human resources, sizing, checkpoint, feedback, and incidents.

and screener effectiveness measures. TSA has not yet fully established its methodology for developing the indexes, but it expects to have the indexes developed by the end of fiscal year 2004.

In conjunction with measuring the performance of its passenger screening operations, TSA must also assess the performance of the five pilot airports that are currently using contract screeners to determine the feasibility of using private screening companies instead of federal screeners.[13] Although ATSA allows airports to apply to opt out of using federal screeners beginning in November 2004, TSA has not yet determined how to evaluate and measure the performance of the pilot program. In early October 2003, TSA awarded a contract to BearingPoint, Inc., to compare the performance of pilot screening with federal screening, including the overall strengths and weaknesses of both systems, and determine the reasons for any differences.[14] The evaluation is scheduled to be completed by March 31, 2004.[15] TSA has acknowledged that designing an effective evaluation of the screeners at the pilot airports will be challenging because key operational areas, including training, assessment, compensation, and equipment, have to a large extent been held constant across all airports, and therefore are not within the control of the private screening companies.[16] In its request for proposal for the pilot airport evaluation, TSA identified several data sources for the evaluation, including the Performance Management Information System and the Office of Internal Affairs and Program Review's covert testing of passenger screeners. However, as we recently reported, data from both of these systems in measuring the effectiveness of screening operations is limited. As a result, it will be a challenge for TSA to effectively compare the performance of

[13]ATSA requires TSA to implement a pilot program using contract screeners at five commercial airports—one in each of the five airport categories. The purpose of the pilot program is to determine the feasibility of using private screening companies rather than federal screeners.

[14]According to the August 8, 2003, request for quotation for the evaluation of the contract screening pilot program, BearingPoint must include informed performance comparisons, both quantitative and qualitative, of private versus federal screeners overall and within different sizes and categories of airports.

[15]Based on the time frames established in the request for quotation, BearingPoint, Inc. is required to develop a project plan and evaluation model no later than December 12, 2003.

[16]TSA's request for proposal for the pilot program evaluation notes that there are a significant number of operational and managerial elements at the discretion of the private screening companies that should be considered in the evaluation, including supervision, overhead, materials, recruiting, and scheduling.

the contract pilot airports with the performance of airports using federal screeners.

TSA Is Developing Performance Evaluation Tools

TSA has recognized the need to strengthen the assessment of its performance, and has initiated efforts to develop and implement strategic and performance plans to clarify goals, establish performance measures, and measure the performance of its security initiatives. Strategic plans are the starting point for an agency's planning and performance measurement efforts. Strategic plans include a comprehensive mission statement based on the agency's statutory requirements, a set of outcome-related strategic goals, and a description of how the agency intends to achieve these goals. The Government Performance and Results Act (GPRA)[17] establishes a framework for strategic plans that requires agencies to

- clearly establish results-oriented performance goals in strategic and annual performance plans for which they will be held accountable,
- measure progress toward achieving those goals,
- determine the strategies and resources to effectively accomplish the goals,
- use performance information to make programmatic decisions necessary to improve performance, and
- formally communicate results in performance reports.

Although the Department of Homeland Security plans to issue one strategic plan for the Department, it plans to incorporate strategic planning efforts from each of its component agencies. TSA recently completed a draft of its input into the Department of Homeland Security's strategic plan. TSA officials stated that the draft is designed to ensure their

[17]The Government Performance and Results Act of 1993 shifts the focus of government operations from process to results by establishing a foundation for examining agency mission, performance goals and objectives, and results. Under the Act, agencies are to prepare 5-year strategic plans that set the general direction for their efforts, and annual performance plans that establish connections between the long-term strategic goals outlined in the strategic plans and the day-to-day activities of managers and staff. Finally, the Act requires that each agency report annually on the extent to which it is meeting its annual performance goals and the actions needed to achieve or modify those goals that have not been met.

security initiatives are aligned with the agency's goals and objectives, and that these initiatives represent the most efficient use of their resources. TSA officials submitted the draft plan to stakeholders in September 2003 for their review and comment. The Department of Homeland Security plans to issue its strategic plan by the end of the year.[18]

In addition to developing a strategic plan, TSA is developing a performance plan to help it evaluate the current effectiveness and levels of improvement in its programs, based on established performance measures. TSA submitted to the Congress a short-term performance plan in May 2003, as required by ATSA, that included performance goals and objectives. The plan also included an initial set of 32 performance measures, including the percentage of bags screened by explosive detection systems and the percentage of screeners in compliance with training standards. However, these measures were primarily output-based (measuring whether specific activities were achieved) and did not measure the effectiveness of TSA's security initiatives. TSA officials acknowledge that the goals and measures included in the report were narrowly focused, and that in moving forward additional performance-based measures are needed.

In addition to developing a short-term performance plan, ATSA also requires that TSA develop a 5-year performance plan and annual performance report, including an evaluation of the extent to which its goals and objectives were met. TSA is currently developing performance goals and measures as part of its annual planning process and will collect baseline data throughout fiscal year 2004 to serve as a foundation for its performance targets. TSA also plans to increase its focus on measuring the effectiveness of various aspects of the aviation security system in its 5-year performance plan. According to TSA's current draft strategic plan, which outlines its overall goals and strategies for fiscal years 2003 through

[18]TSA is also developing a National Transportation Security System Plan, a draft of which is currently under review within TSA. TSA plans to promote consistent and mutually supporting intermodal planning in cooperation with administrators and in collaboration with key stakeholders from all modes of transportation. TSA designed the plan for use by agencies, owners, and operators of the transportation system to guide them as they develop their individual security plans. Accordingly, the National Transportation System Security Plan will include national modal plans to capture and tailor transportation security requirements for each mode of transportation, with particular emphasis on intermodal connections. Each modal plan will focus on security for people (workforce and passengers), cargo (baggage and shipments), infrastructure (vehicles, facilities, and right of ways), and response preparedness.

2008, its efforts to measure the effectiveness of the aviation security system will include

- random and scheduled reviews of the efficiency and effectiveness of security processes;
- oversight of compliance with security standards and approved programs through a combination of inspections, testing, interviews, and record reviews—to include TIP;
- measurement of performance against standards to ensure expected standards are met and to drive process improvements; and
- collection and communication of performance data using a state-of-the-art data collection and reporting system.

In our January 2003 report on TSA's actions and plans to build a results-oriented culture, we recommended next steps that TSA should take to strengthen its strategic planning efforts.[19] These steps include establishing security performance goals and measures for all modes of transportation that involves stakeholders, and applying practices that have been shown to provide useful information in agency performance plans. We also identified practices that TSA can apply to ensure the usefulness of its required 5-year performance plan to TSA managers, the Congress, and other decision makers or interested parties. Table 1 outlines the practices we identified for TSA.

[19] U.S. General Accounting Office, *Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture*, GAO-03-190 (Washington, D.C.: Jan. 17, 2003).

Table 1: Summary of Opportunities to Help Ensure Useful Annual Plans and Applied Practices

Opportunities to help ensure useful annual plans	Applied practices
Articulate a results orientation	1. Create a set of performance goals and measures that addresses important dimensions of program performance and balances competing priorities. 2. Use intermediate goals and measures to show progress or contribution to intended results. 3. Include explanatory information on the goals and measures. 4. Develop performance goals to address mission-critical management problems. 5. Show baseline and trend data for past performance. 6. Identify projected target levels of performance for multiyear goals. 7. Link the goals of component organizations to departmental strategic goals.
Coordinate cross-cutting programs	8. Identify programs that contribute to the same or similar results. 9. Set complementary performance goals to show how differing program strategies are mutually reinforcing and establish common or complementary performance measures, as appropriate. 10. Describe—briefly or refer to a separate document—planned coordination strategies.
Show how strategies will be used to achieve goals	11. Link strategies and programs to specific performance goals and describe how they will contribute to the achievement of those goals. 12. Describe strategies to leverage or mitigate the effects of external factors on the accomplishment of performance goals. 13. Discuss strategies to resolve mission-critical management problems. 14. Discuss—briefly or refer to a separate plan—plans to ensure that mission-critical processes and information systems function properly and are secure.
Show performance consequences of budget and other resource decisions	15. Show how budgetary resources relate to the achievement of performance goals. 16. Discuss—briefly and refer to the agency capital plan—how proposed capital assets (specifically information technology investments) will contribute to achieving performance goals. 17. Discuss—briefly or refer to a separate plan—how the agency will use its human capital.
Build the capacity to gather and use performance information	18. Identify internal and external sources of data. 19. Describe efforts to verify and validate performance data. 20. Identify actions to compensate for unavailable or low-quality data. 21. Discuss implications of data limitations for assessing performance.

Source: GAO.

TSA agreed with our recommendation and plans to incorporate these principles into the data it provides DHS for the department's 5-year performance plan and annual performance report. DHS plans to complete its 5-year performance plan and annual performance report by February 2004, as required by GPRA.

The Congress has also recognized the need for TSA to collect performance data and, as part of the Federal Aviation Administration's (FAA) reauthorization act—Vision 100: Century of Aviation Reauthorization Act—is currently considering a provision that would require the Secretary of the Department of Homeland Security to conduct a study of the effectiveness of the aviation security system.

Risk Management Approach Needed To Focus Security Efforts

As TSA moves forward in addressing aviation security concerns, it needs adequate tools to ensure that its efforts are appropriately focused, strategically sound, and achieving expected results. Because of limited funding, TSA needs to set priorities so that its resources can be focused and directed to those aviation security enhancements most in need of implementation. In recent years, we have consistently advocated the use of a risk management approach to respond to various national security and terrorism challenges, and have recommended that TSA apply this approach to strengthen security in aviation as well as in other modes of transportation.[20] TSA agreed with our recommendation and is adopting a risk management approach.

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 1 describes the risk management approach.

[20]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001); and GAO-03-344.

Figure 1: 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.

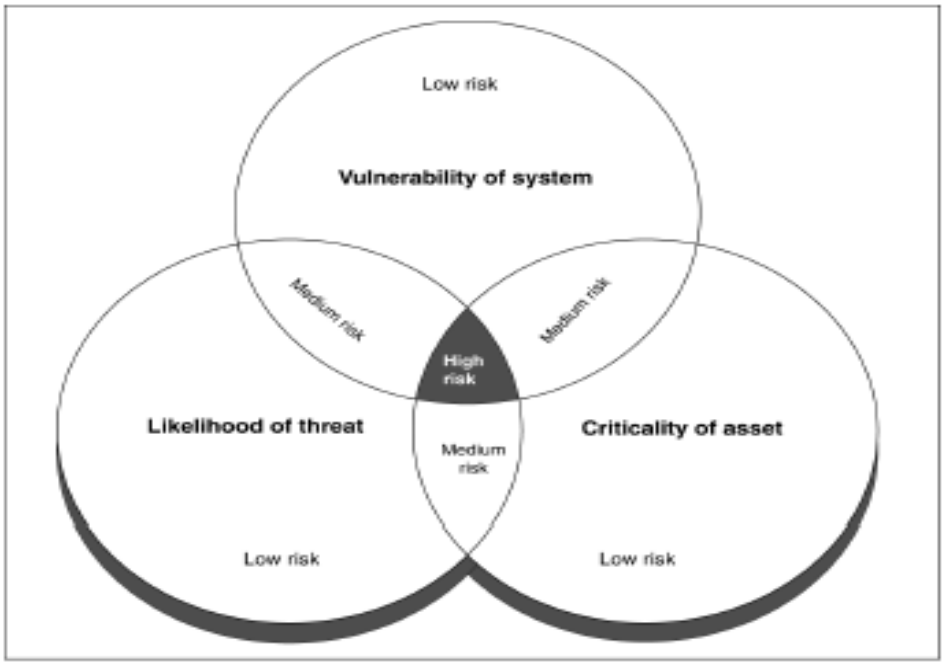
A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses. In general, a vulnerability assessment is conducted by a team of experts skilled in such areas as engineering, intelligence, security, information systems, finance, 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 2 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 2: A Risk Management Approach



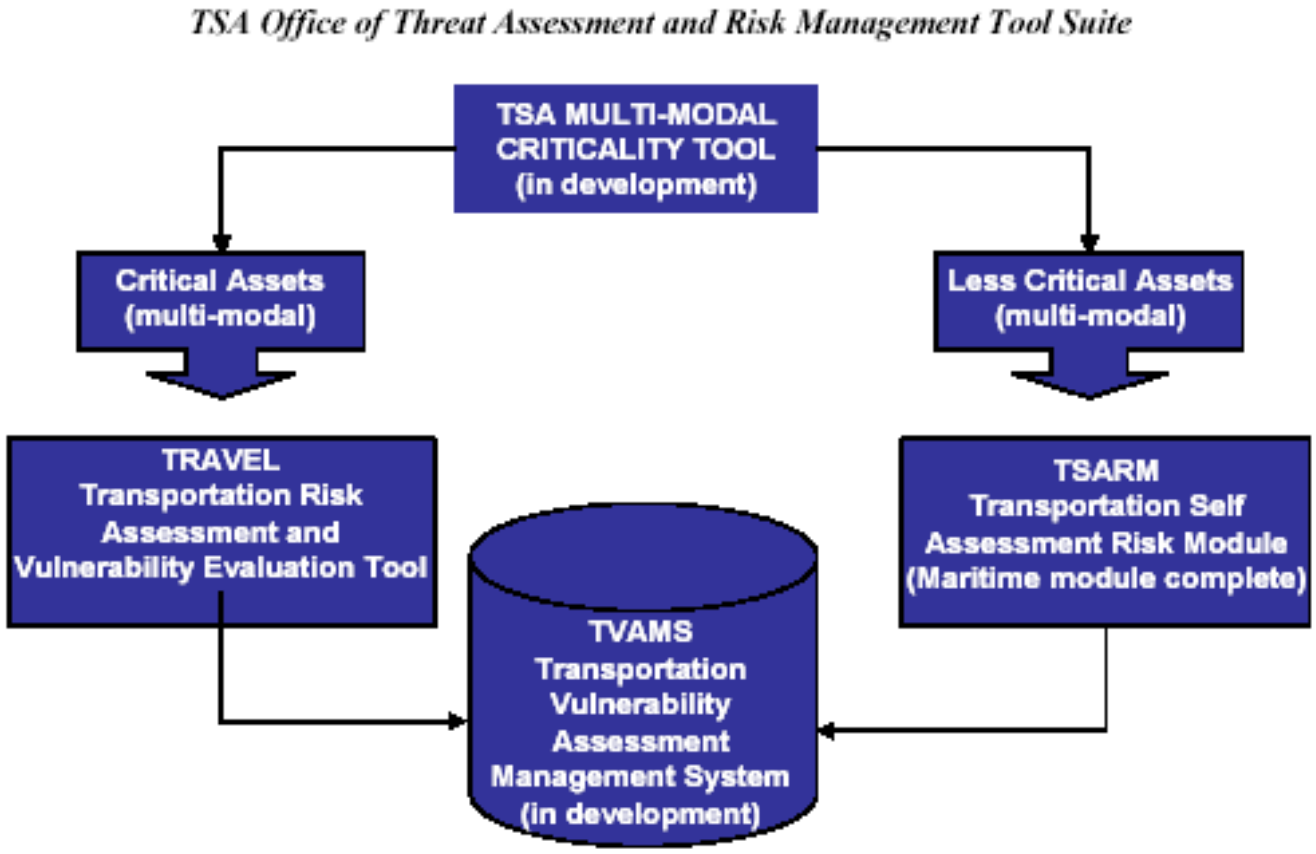
Source: GAO.

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.

Over the past several years, we have concluded that comprehensive threat, vulnerability, and criticality assessments are key in better preparing against terrorist attacks, and we have recommended that TSA apply this risk management approach to strengthen security in aviation. TSA agreed with our recommendation and is adopting a risk management approach in an attempt to enhance security across all modes of transportation. According to TSA officials, once established, risk management principles will drive all decisions—from standard setting to funding priorities 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 developing four assessment tools that will help assess threats, criticality, and vulnerabilities. Figure 3 illustrates TSA's threat assessment and risk management approach.

Figure 3: TSA's Risk Management Approach and Tools



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 office—the Information and Analysis Protection Directorate—to ensure that the criticality tool will be consistent with the Department's overall approach for managing critical infrastructure.

A second tool—the Transportation Risk Assessment and Vulnerability Tool (TRAVEL)—will assess threats and analyze vulnerabilities at those transportation assets TSA determines to be nationally critical. The tool will be used in a TSA-led and facilitated assessment that will be conducted on the site of the transportation asset.[21] Specifically, the tool will assess an asset's baseline security system and that system's effectiveness in detecting, deterring, and preventing various threat scenarios, and it will produce a relative risk score for potential attacks against a transportation asset or facility. 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 when the threat level increases. For example, as the threat level increases from yellow to orange, as determined by the Department of Homeland Security, the assessment tool might advise an entity to take increased security measures, such as erecting barriers and closing selected entrances. TSA

[21]A vulnerability assessment using the TRAVEL tool requires the participation of TSA subject matter experts along with representatives from the transportation asset. Operations management, facilities management, security personnel, and law enforcement agents are examples of the individuals involved in analyzing each threat scenario and corresponding security system.

had deployed one self-assessment module in support of targeted maritime vessel and facility categories.[22]

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 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.

TSA is now using components of these risk management tools and is automating others so that the components can be used remotely by stakeholders, such as small airports, to assess their risks. For example, according to TSA officials, TSA has conducted assessments at 9 of 443 commercial airports using components of its TRAVEL tool. Three of these assessments were conducted at category X airports (the largest and busiest airports), and the remaining 6 assessments were conducted at airports in lower categories. TSA plans to conduct approximately 100 additional assessments of commercial airports in 2004 using TRAVEL and plans to begin compiling data on security vulnerability trends in 2005. Additionally, TSA plans to fully implement and automate its risk management approach by September 2004.

TSA Faces Additional Programmatic And Management Challenges

In addition to collecting performance data and implementing a risk management approach, TSA faces a number of other programmatic and management challenges in strengthening aviation security. These challenges include implementing the new Computer-Assisted Passenger Prescreening System; strengthening baggage screening, airport perimeter and access controls, air cargo, and general aviation security; managing the costs of aviation security initiatives; and managing human capital. TSA has been addressing these challenges through a variety of efforts. We have work in progress that is examining TSA's efforts in most of these areas, and we will be reporting on TSA's progress in the future.

[22]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 United States Coast Guard by January 1, 2004.

Computer-Assisted Passenger Prescreening System (CAPPS II)

ATSA authorized TSA to develop a new Computer-Assisted Passenger Prescreening System, or CAPPS II. This system is intended to replace the current Computer-Assisted Passenger Screening program, which was developed in the mid-1990s by the Federal Aviation Administration to enable air carriers to identify passengers requiring additional security attention. The current system is maintained as a part of the airlines' reservation systems and, operating under federal guidelines, uses a number of behavioral characteristics to select passengers for additional screening.

In the wake of the September 11, 2001, terrorist attacks, a number of weaknesses in the current prescreening program were exposed. For example, although the characteristics used to identify passengers for additional screening are classified, several have become public knowledge through the press or on the Internet. Although enhancements have been made to address some of these weaknesses, the behavioral traits used in the system may not reflect current intelligence information. It is also difficult to quickly modify the system to respond to real-time changes in threats. Additionally, because the current system operates independently within each air carrier reservation system, changes to each air carrier's system to modify the prescreening system can be costly and time-consuming.

In contrast, CAPPS II is planned to be a government-run program that will provide real–time risk assessment for all airline passengers. Unlike the current system, TSA is designing CAPPS II to identify and compare personal information with commercially available data to confirm a passenger's identity. The system will then run the identifying information against government databases and generate a "risk" score for the passenger. The risk score will determine the level of screening that the passenger will undergo before boarding. TSA currently estimates that initial implementation of CAPPS II will occur during the fall of 2004, with full implementation expected by the fall of 2005.

TSA faces a number of challenges that could impede their ability to implement CAPPS II. Among the most significant are the following:

- concerns about travelers' privacy rights and the safeguards established to protect passenger data;
- the accuracy of the databases being used by the CAPPS II system and whether inaccuracies could generate a high number of false positives

and erroneously prevent or delay passengers from boarding their flights;

- the length of time that data will be retained by TSA;
- the availability of a redress process through which passengers could get erroneous information corrected;
- concerns that identify theft, in which someone steals relevant data and impersonates another individual to obtain that person's low risk score, may not be detected and thereby negate the security benefits of the system; and
- obtaining the international cooperation needed for CAPPS II to be fully effective, as some countries consider the passenger information required by CAPPS II as a potential violation of their privacy laws.

We are currently assessing these and other challenges in the development and implementation of the CAPPS II system and expect to issue a final report on our work in early 2004.

Checked Baggage Screening

Checked baggage represents a significant security concern, as explosive devices in baggage can, and have, been placed in aircraft holds. ATSA required screening of all checked baggage on commercial aircraft by December 31, 2002, using explosive detection systems to electronically scan baggage for explosives. According to TSA, electronic screening can be accomplished by bulk explosives detection systems (EDS)[23] or Explosives Trace Detection (ETD) systems.[24] However, TSA faced challenges in meeting the mandated implementation date. First, the production capabilities of EDS manufacturers were insufficient to produce the number of units needed. Additionally, according to TSA, it was not possible to undertake all of the airport modifications necessary to accommodate the EDS equipment in each airport's baggage handling area. In order to ensure that all checked baggage is screened, TSA established a

[23]Explosives detection systems use probing radiation to examine objects inside baggage and identify the characteristic signatures of threat explosives. EDS equipment operates in an automated mode.

[24]Explosive trace detection works by detecting vapors and residues of explosives. Human operators collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosive materials.

program that uses alternative measures, including explosives sniffing dogs, positive passenger bag match,[25] and physical hand searches at airports where sufficient EDS or ETD technology is not available. TSA was granted an extension for screening all checked baggage electronically, using explosives detection systems, until December 31, 2003.

Although TSA has made progress in implementing EDS technology at more airports, it has reported that it will not meet the revised mandate for 100 percent electronic screening of all checked baggage. Specifically, as of October 2003, TSA reported that it will not meet the deadline for electronic screening by December 31, 2003, at five airports. Airport representatives with whom we spoke expressed concern that there has not been enough time to produce, install, and integrate all of the systems required to meet the deadline.

In addition to fielding the EDS systems at airports, difficulties exist in integrating these systems into airport baggage handling systems. For those airports that have installed EDS equipment, many have been located in airport lobbies as stand-alone systems. The chief drawback of stand-alone systems is that because of their size and weight there is a limit to the number of units that can be placed in airport lobbies, and numerous screeners are required to handle the checked bags because each bag must be physically conveyed to the EDS machines and then moved back to the conveyor system for transport to the baggage handling room in the air terminal. Some airports are in the process of integrating the EDS equipment in-line with the conveyor belts that transport baggage from the ticket counter to the baggage handling area; however, the reconfiguring of airports for in-line checked baggage screening can be extensive and costly.[26] TSA has reported that in-line EDS equipment installation costs range from $1 million to $3 million per piece of equipment. In February 2003, we identified letters of intent[27] as a funding option that has been

[25]Positive passenger bag match is an alternative method of screening checked baggage, which requires that the passenger be on the same aircraft as the checked baggage.

[26]In-line screening involves incorporating EDS machines into airport baggage handling systems to improve throughput of baggage and to streamline airport operations.

[27]A letter of intent represents a nonbinding commitment from an agency to provide multiyear funding to an entity beyond the current authorization period. Thus, that letter allows an airport to proceed with a project without waiting for future federal funds because the airport and investors know that allowable costs are likely to be reimbursed.

successfully used to leverage private sources of funding.[28] TSA has since written letters of intent covering seven airports promising multiyear financial support totaling over $770 million for in-line integration of EDS equipment.[29] Further, TSA officials have stated that they have identified 25 to 35 airports as candidates for further letters of intent pending Congressional authorization of funding. We are examining TSA's baggage screening program, including its issuance of letters of intent, in an ongoing assignment.

Perimeter and Access Controls

Prior to September 2001, work performed by GAO, and others, highlighted the vulnerabilities in controls for limiting access to secure airport areas. In one report, we noted that GAO special agents were able to use fictitious law enforcement badges and credentials to gain access to secure areas, bypass security checkpoints, and walk unescorted to aircraft departure gates.[30] The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. Concerns over the adequacy of the vetting process for airport workers who have unescorted access to secure airport areas have also arisen, in part, as a result of federal agency airport security sweeps that uncovered hundreds of instances in which airport workers lied about their criminal history, or immigration status, or provided false or inaccurate Social Security numbers on their application for security clearances to obtain employment.

ATSA contains provisions to improve perimeter access security at the nation's airports and strengthen background checks for employees working in secure airport areas, and TSA has made some progress in this area. For example, federal mandates were issued to strengthen airport perimeter security by limiting the number of airport access points, and

[28]U.S. General Accounting Office, *Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development*, GAO-03-497T (Washington, D.C.: Feb. 25, 2003).

[29]The seven airports include Denver International Airport, Las Vegas McCarran International Airport, Los Angeles International Airport, Ontario International Airport, Seattle/Tacoma International Airport, Dallas/Fort Worth International Airport, and Boston Logan International Airport. The purpose is to help defray the costs of installing permanent explosive detection systems that are integrated with airports' checked baggage conveyor systems.

[30]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO\T-OSI-00-10 (Washington, D.C.: May 25, 2000).

they require random screening of individuals, vehicles, and property before entry at the remaining perimeter access points. Further, TSA made criminal history checks mandatory for employees with access to secure or sterile airport areas. To date, TSA has conducted approximately 1 million of these checks. TSA also has plans to develop a pilot airport security program and is reviewing security technologies in the areas of biometrics access control identification systems (i.e., fingerprints or iris scans), anti-piggybacking technologies (to prevent more than one employee from entering a secure area at a time), and video monitoring systems for perimeter security. TSA solicited commercial airport participation in the program. It is currently reviewing information from interested airports and plans to select 20 airports for the program.

Although progress has been made, challenges remain with perimeter security and access controls at commercial airports. Specifically, ATSA contains numerous requirements for strengthening perimeter security and access controls, some of which contained deadlines, which TSA is working to meet. In addition, a significant concern is the possibility of terrorists using shoulder-fired portable missiles from locations near the airport. We reported in June 2003 that airport operators have increased their patrols of airport perimeters since September 2001, but industry officials stated that they do not have enough resources to completely protect against missile attacks.[31] A number of technologies could be used to secure and monitor airport perimeters, including barriers, motion sensors, and closed-circuit television. Airport representatives have cautioned that as security enhancements are made to airport perimeters, it will be important for TSA to coordinate with the Federal Aviation Administration and the airport operators to ensure that any enhancements do not pose safety risks for aircraft. To further examine these threats and challenges, we have ongoing work assessing TSA's progress in meeting ATSA provisions related to improving perimeter security, access controls, and background checks for airport employees and other individuals with access to secure areas of the airport, as well as the nature and extent of the threat from shoulder-fired missiles.

Air Cargo Security

As we and the Department of Transportation's Inspector General have reported, vulnerabilities exist in ensuring the security of cargo carried

[31]U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003).

aboard commercial passenger and all-cargo aircraft. TSA has reported that an estimated 12.5 million tons of cargo are transported each year—9.7 million tons on all-cargo planes and 2.8 million tons on passenger planes. Potential security risks are associated with the transport of air cargo—including the introduction of undetected explosive and incendiary devices in cargo placed aboard aircraft. To reduce these risks, ATSA requires that all cargo carried aboard commercial passenger aircraft be screened and that TSA have a system in place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo on all-cargo aircraft. Despite these requirements, it has been reported that less than 5 percent of cargo placed on passenger airplanes is physically screened.[32] TSA's primary approach to ensuring air cargo security and safety is to ensure compliance with the "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders to ship cargo on planes. However, we and the Department of Transportation's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders, such as possible tampering with freight at various handoff points before it is loaded into an aircraft.[33]

Since September 2001, TSA has taken a number of actions to enhance cargo security, such as implementing a database of known shippers in October 2002. The database is the first phase in developing a cargo profiling system similar to the Computer-Assisted Passenger Prescreening System. However, in December 2002, we reported that additional operational and technological measures, such as checking the identity of individuals making cargo deliveries, have the potential to improve air cargo security in the near term.[34] We further reported that TSA lacks a comprehensive plan with long-term goals and performance targets for cargo security, time frames for completing security improvements, and risk-based criteria for prioritizing actions to achieve those goals. Accordingly, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation and expects to develop such a plan by

[32]Congressional Research Service, *Air Cargo Security*, September 11, 2003.

[33]U.S. General Accounting Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344 (Washington, D.C.: Dec. 20, 2002).

[34]See footnote 33.

the end of 2003. It will be important that this plan include a timetable for implementation to help ensure that vulnerabilities in this area are reduced.

General Aviation Security

Since September 2001, TSA has taken limited action to improve general aviation security, leaving general aviation far more open and potentially vulnerable than commercial aviation. General aviation is vulnerable because general aviation pilots and passengers are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports.[35] More than 550 of these airports also provide commercial service. In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists. This vulnerability was demonstrated in January 2002, when a teenage flight student stole and crashed a single-engine airplane into a Tampa, Florida skyscraper. Moreover, general aviation aircraft could be used in other types of terrorist acts. It was reported that the September 11th hijackers researched the use of crop dusters to spread biological or chemical agents.

We reported in September 2003 that TSA chartered a working group on general aviation within the existing Aviation Security Advisory Committee.[36] The working group consists of industry stakeholders and is designed to identify and recommend actions to close potential security gaps in general aviation. On October 1, 2003, the working group issued a report that included a number of recommendations for general aviation airport operators' voluntary use in evaluating airports' security requirements. These recommendations are both broad in scope and generic in their application, with the intent that every general aviation airport and landing facility operators may use them to evaluate that facility's physical security, procedures, infrastructure, and resources. TSA is taking some additional action to strengthen security at general aviation airports, including developing a risk-based self-assessment tool for general

[35]Of the 19,000 general aviation airports, 5,400 are publicly owned. TSA is currently focusing its efforts on these publicly owned airports. TSA is still unclear about its role in inspecting privately owned general aviation airports.

[36]U.S. General Accounting Office, *Aviation Security: Progress since Septermber 11th, and the Challenges Ahead*, GAO-03-1150T (Washington, D.C.: September 9, 2003).

aviation airports to use in identifying security concerns. We have ongoing work that is examining general aviation security in further detail.

Aviation Security Funding

TSA faces two key funding and accountability challenges in securing the commercial aviation system: (1) paying for increased aviation security and (2) ensuring that these costs are controlled. The costs associated with the equipment and personnel needed to screen passengers and their baggage alone are huge. The Department of Homeland Security appropriation includes $3.7 billion for aviation security for fiscal year 2004, with about $1.8 billion for passenger screening and $1.3 billion for baggage screening. ATSA created a passenger security fee to pay for the costs of aviation security, but the fee has not generated enough money to do so. The Department of Transportation's Inspector General reported that the security fees are estimated to generate only about $1.7 billion during fiscal year 2004.

A major funding challenge is paying for the purchase and installation of the remaining explosives detection systems, including integration into airport baggage-handling systems. Integrating the equipment with the baggage-handling systems is expected to be costly because it will require major facility modifications. For example, modifications needed to integrate the equipment at Boston's Logan International Airport are estimated to cost $146 million. Modifications for Dallas/Fort Worth International Airport are estimated to cost $193 million. According to TSA and the Department of Transportation's Inspector General, the cost of integrating the equipment nationwide could be $3 billion.

A key question that must be addressed is how to pay for these installation costs. The Federal Aviation Administration's Airport Improvement Program (AIP) and passenger facility charges have been eligible sources for funding this work.[37] During fiscal year 2002, AIP grant funds totaling $561 million were used for terminal modifications to enhance security. However, using these funds for security reduced the funding available for other airport development and rehabilitation projects. To provide financial assistance to airports for security-related capital investments, such as the installation of explosives detection equipment, proposed aviation

[37]The Airport Improvement Program trust fund is used to fund capital improvements to airports, including some security enhancements, such as terminal modifications to accommodate explosive detection equipment.

reauthorization legislation would establish an aviation security capital fund that would authorize $2 billion over the next 4 years. The funding would be made available to airports in letters of intent, and large and medium hub airports would be expected to provide a match of 10 percent of a project's costs. A 5 percent match would be required for all other airports.

In February 2003, we identified letters of intent as a funding option that has been successfully used to leverage private sources of funding.[38] TSA has since signed letters of intent covering seven airports—Boston Logan, Dallas/Fort Worth, Denver, Los Angeles, McCarran (Las Vegas), Ontario (California), and Seattle/Tacoma international airports. Under the agreements, TSA will pay 75 percent of the cost of integrating the explosives detection equipment into the baggage-handling systems. The payments will stretch out over 3 to 4 years. TSA officials have identified more airports that would be candidates for similar agreements.

Another challenge is ensuring continued investment in transportation research and development. For fiscal year 2003, TSA was appropriated about $110 million for research and development, of which $75 million was designated for the next-generation explosives detection systems. However, TSA proposed to reprogram $61.2 million of these funds to be used for other purposes, leaving about $12.7 million to be spent on research and development in that year. This proposed reprogramming could limit TSA's ability to sustain and strengthen aviation security by continuing to invest in research and development for more effective equipment to screen passengers, their carry-on and checked baggage, and cargo. In ongoing work, we are examining the nature and scope of research and development work by TSA and the Department of Homeland Security, including their strategy for accelerating the development of transportation security technologies.

Human Capital Management

As it organizes itself to protect the nation's transportation system, TSA faces the challenge of strategically managing its workforce of about 60,000 people—more than 80 percent of whom are passenger and baggage screeners. Additionally, over the next several years, TSA faces the

[38]U.S. General Accounting Office, *Airport Financing: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development*, GAO-03-497T (Washington, D.C.: Feb. 25, 2003).

challenge of sizing and managing this workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures. For example, as explosives detection systems are integrated with baggage-handling systems, the use of more labor-intensive screening methods, such as trace detection techniques and manual bag searches, can be reduced. Other planned security enhancements, such as CAPPS II and the registered traveler program, also have the potential to make screening more efficient. Further, if airports opt out of the federal screener program and use their own or contract employees to provide screening instead of TSA screeners, a significant impact on TSA staffing could occur.

To assist agencies in managing their human capital more strategically, we have developed a model that identifies cornerstones and related critical success factors that agencies should apply and steps they can take.[39] Our model is designed to help agency leaders effectively lead and manage their people and integrate human capital considerations into daily decision making and the program results they seek to achieve. In January 2003, we reported that TSA was addressing some critical human capital success factors by using a wide range of tools available for hiring, and beginning to link individual performance to organizational goals.[40] However, concerns remain about the size and training of that workforce, the adequacy of the initial background checks for screeners, and TSA's progress in setting up a performance management system. TSA is currently developing a human capital strategy, which it expects to be completed by the end of this year.

TSA has proposed cutting the screener workforce by an additional 3,000 during fiscal year 2004. This planned reduction has raised concerns about passenger delays at airports and has led TSA to begin hiring part-time screeners to make more flexible and efficient use of its workforce. In addition, TSA used an abbreviated background check process to hire and deploy enough screeners to meet ATSA's screening deadlines during 2002. After obtaining additional background information, TSA terminated the employment of some of these screeners. TSA reported 1,208 terminations as of May 31, 2003, that it ascribed to a variety of reasons, including criminal offenses and failures to pass alcohol and drug tests. Furthermore, the national media have reported allegations of operational and

[39]U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: March 2002).

[40]U.S. General Accounting Office, Transportation *Security Administration: Actions and Plans to Build a Results-Oriented Culture*, GAO-03-190 (Washington, D.C.: Jan. 13, 2003).

management control problems that emerged with the expansion of the Federal Air Marshal Service, including inadequate background checks and training, uneven scheduling, and inadequate policies and procedures. We reported in January 2003 that TSA had taken the initial steps in establishing a performance management system linked to organizational goals. Such a system will be critical for TSA to motivate and manage staff, ensure the quality of screeners' performance, and, ultimately, restore public confidence in air travel. In ongoing work, we are examining the effectiveness of TSA's efforts to train, equip, and supervise passenger screeners, and we are assessing the effects of expansion on the Federal Air Marshal Service.[41]

Concluding Observations

As TSA moves forward in addressing aviation security concerns, it needs the information and tools necessary to ensure that its efforts are appropriately focused, strategically sound, and achieving expected results. Without knowledge about the effectiveness of its programs and a process for prioritizing planned security initiatives, TSA and the public have little assurance regarding the level of security provided, and whether TSA is using its resources to maximize security benefits. Additionally, as TSA implements new security initiatives and addresses associated challenges, measuring program effectiveness and prioritizing efforts will help it focus on the areas of greatest importance. We are encouraged that TSA is undertaking efforts to develop the information and tools needed to measure its performance and focus its efforts on those areas of greatest need.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have.

[41]The Federal Air Marshal Service has been transferred out of TSA and into the Department of Homeland Security's Bureau of Immigration and Customs Enforcement.

Contact Information

For further information on this testimony, please contact Cathleen A. Berrick at (202) 512-8777. Individuals making key contributions to this testimony include Mike Bollinger, Lisa Brown, Jack Schulze, Maria Strudwick, and Susan Zimmerman.

Related GAO Products

Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining. GAO-03-1173. Washington, D.C.: September 24, 2003.

Aviation Security: Progress since September 11, 2001, and the Challenges Ahead. GAO-03-1150T. Washington, D.C.: September 9, 2003

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO-03-843. Washington, D.C.: June 30, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process. GAO-03-248NI. Washington, D.C.: February 3, 2003 (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-286NI. Washington, D.C.: December 20, 2002 (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-344. Washington, D.C.: December 20, 2002.

Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods. GAO-03-30C. Washington, D.C.: December 3, 2002

Aviation Security: Registered Traveler Program Policy and Implementation Issues. GAO-03-253. Washington, D.C.: November 22, 2002.

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges. GAO-03-971T. Washington, D.C.: July 25, 2002.

Aviation Security: Information Concerning the Arming of Commercial Pilots. GAO-02-822R. Washington, D.C.: June 28, 2002.

Aviation Security: Deployment and Capabilities of Explosive Detection Equipment. GAO-02-713C. Washington, D.C.: June 20, 2002 (CLASSIFIED).

Aviation Security: Information on Vulnerabilities in the Nation's Air Transportation System. GAO-01-1164T. Washington, D.C.: September 26, 2001 (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Information on the Nation's Air Transportation System Vulnerabilities. GAO-01-1174T. Washington, D.C.: September 26, 2001 (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations. GAO-01-1171T. Washington, D.C.: September 25, 2001.

Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities. GAO-01-1165T. Washington, D.C.: September 21, 2001.

Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports. GAO-01-1162T. Washington, D.C.: September 20, 2001.

Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security. GAO-01-1166T. Washington, D.C.: September 20, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1069R. Washington, D.C.: August 31, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1068R. Washington, D.C.: August 31, 2001 (RESTRICTED).

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

Aviation Security: Additional Controls Needed to Address Weaknesses in Carriage of Weapons Regulations. GAO/RCED-00-181. Washington, D.C.: September 29, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

FAA Computer Security: Concerns Remain due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance. GAO/RCED-00-75. Washington, D.C.: June 28, 2000.

Aviation Security: Screeners Continue to Have Serious Problems Detecting Dangerous Objects. GAO/RCED-00-159. Washington, D.C.: June 22, 2000 (NOT FOR PUBLIC DISSEMINATION).

Security: Breaches at Federal Agencies and Airports. GAO-OSI-00-10. Washington, D.C.: May 25, 2000.

Aviation Security: Screener Performance in Detecting Dangerous Objects during FAA Testing Is Not Adequate. GAO/T-RCED-00-143. Washington, D.C.: April 6, 2000 (NOT FOR PUBLIC DISSEMINATION).

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548