S. HRG. 108–999

AVIATION SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

NOVEMBER 5, 2003

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

20–547 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina, *Ranking*
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN D. ROCKEFELLER IV, West Virginia
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	BYRON L. DORGAN, North Dakota
GORDON H. SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	BARBARA BOXER, California
JOHN ENSIGN, Nevada	BILL NELSON, Florida
GEORGE ALLEN, Virginia	MARIA CANTWELL, Washington
JOHN E. SUNUNU, New Hampshire	FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

CONTENTS

AVIATION SECURITY

WEDNESDAY, NOVEMBER 5, 2003

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:48 a.m. in room SR–253, Russell Senate Office Building, Hon. John McCain [Chairman], presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. All right, we will begin. We will begin our hearing. We thank the witnesses for their patience and we thank those who are waiting to attend the hearing for their patience.

Ms. Berrick, we will begin with you. Go ahead, and pull the microphone over.

STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

Ms. BERRICK. Thank you. Thank you, Mr. Chairman, and Members of the Committee, for the opportunity to participate in today's hearing to discuss the security of commercial aviation.

It has been 2 years since the attacks of September 11, and since that time, billions of dollars have been spent on a variety of initiatives to enhance security. However, recent reviews and testing conducted by GAO and others, as well as recent media reports, have revealed continuing vulnerabilities in the system.

My testimony today focuses on three areas that we believe were fundamental to TSA's success in enhancing security. These areas include: measuring the effectiveness of TSA's current initiatives, including its passenger screening program; second, fully implementing risk management tools to prioritize future efforts; and third, addressing several key programmatic and management challenges.

I would like to first talk about TSA's efforts to measure the effectiveness of its security initiatives. We found that TSA has collected limited information on the effectiveness of its initiatives, but it is taking steps in the right direction. For example, we recently reported that TSA's primary source of information on the effectiveness of its passenger screening program is through covert testing conducted at security checkpoints. However, we reported that TSA had only tested about 1 percent of its screening workforce.

We also reported that another key source of performance data, the threat image projection system, or TIP, was deactivated after September 11 and has not fully been redeployed. TIP places images of threat objects on an X-ray machine, X-ray screen, during actual operations to record whether or not a screener detects a threat.

We also found that TSA had not fully deployed an annual screener certification program that will provide additional performance data.

As I mentioned, TSA is taking a number of actions to collect more performance data on their programs, including increasing its number of covert testings, actually doubling it, reactivating TIP at all airports by 2004, and they are establishing an annual screener certification program. We are encouraged by these steps and believe that TSA should continue to enhance their performance measurement efforts.

In addition to measuring the effectiveness of security initiatives, we believe that TSA must fully implement risk management tools to prioritize its future efforts. The purpose of a risk management approach is to set priorities so that resources can be focused on the most needed security enhancements. Using this approach to prioritize efforts is especially important due to TSA's responsibility for securing all modes of transportation. TSA has agreed with our past recommendations to implement such an approach and they plan to fully have it implemented by September 2004.

Finally, TSA must overcome some key programmatic and management challenges as they move forward. For example, TSA is developing a new computer-assisted passenger pre-screening system, or CAPPS, to identify passengers who require additional screening. CAPPS will rely on existing data bases to generate a risk score to determine the level of screening that a passenger will undergo.

TSA faces a number of challenges in implementing CAPPS, including addressing concerns regarding the protection of passenger data, the accuracy of data bases being used by CAPPS, and potential identity theft, in which someone steals relevant data and impersonates another individual, thereby negating any security benefits of the system. GAO has an ongoing review of the CAPPS program.

TSA also faces funding and human capital challenges. A significant funding challenge is paying for the integration of explosive detection systems in the airport baggage handling systems, which is estimated to cost from $3 billion to $5 billion over the next 5 years. TSA is also faced with the challenge of appropriately sizing its workforce as efficiencies improve through technology and new processes. For example, as explosive detection systems are integrated with baggage handling systems, the use of more labor-intensive screening methods, such as trace detection and manual bag searches, can be reduced. Other planned enhancements such as CAPPS and the registered traveler program also have the potential to make screening more efficient.

As TSA moves forward in addressing these concerns, it needs the information and tools necessary to ensure that its efforts are appropriately focused and are achieving expected results.

Mr. Chairman, this concludes my opening statement. I would be happy to respond to any questions at the appropriate time.

[The prepared statement of Ms. Berrick follows:]

HIGHLIGHTS

Aviation Security

EFFORTS TO MEASURE EFFECTIVENESS AND ADDRESS CHALLENGES

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.

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 com-

puter-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.

PREPARED STATEMENT OF CATHLEEN A BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

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

---

[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.

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 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 longstanding 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.

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

---

[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.

[5] P.L. No. 107–296.

[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).

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 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 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 Per-

[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.

[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.

formance 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 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 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

---

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

[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.

[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

Continued

- 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 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 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 stra-

---

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.

[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.

tegic 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.

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. 5. 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.

[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).

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.

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.

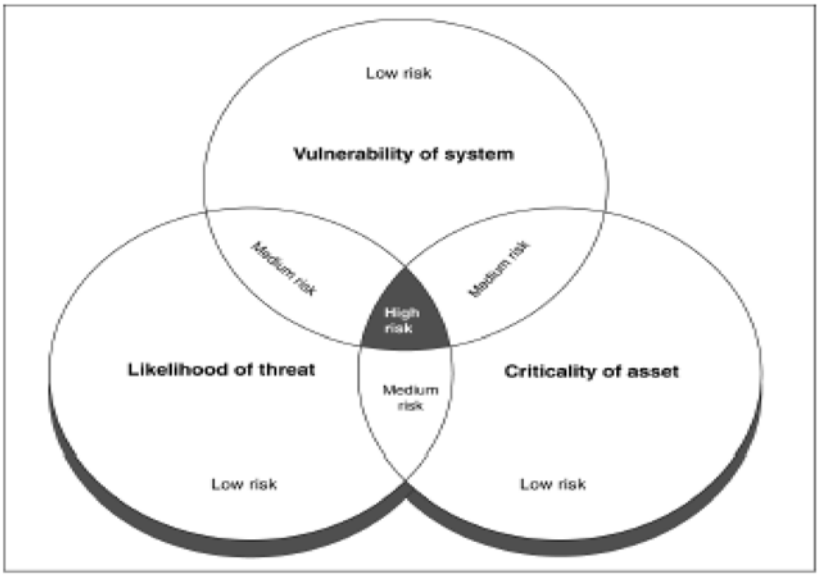
A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such, 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.

[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 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

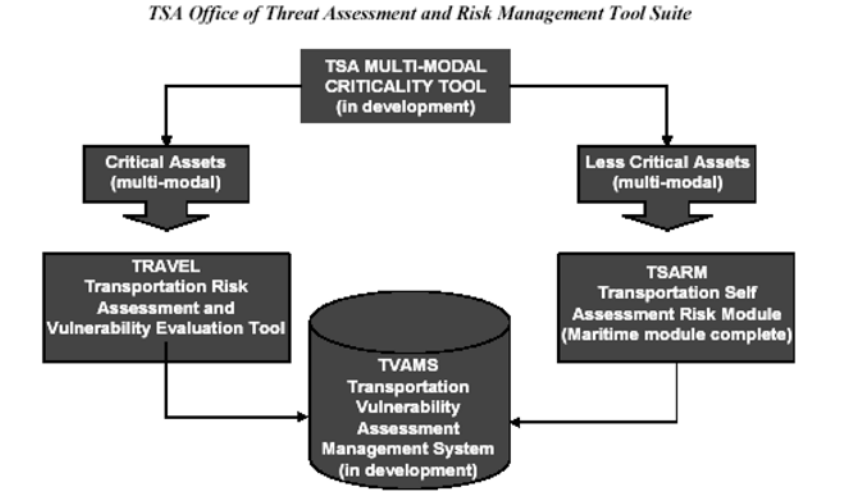


Source: GAO.

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,

[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.

such as erecting barriers and closing selected entrances. TSA 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.

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;

---

[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.

- 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 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 successfully

[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.

[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

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 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.

---

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.

[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).

[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).

Air Cargo Security

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

---

[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.

[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 September 11th, and the Challenges Ahead,* GAO–03–1150T (Washington, D.C.: September 9, 2003).

frastructure, 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 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 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

[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.

[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).

80 percent of whom are passenger and baggage screeners. Additionally, over the next several years, TSA faces the 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 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.

The CHAIRMAN. Thank you very much.
Mr. McHale, do you have an opening statement?
Mr. MCHALE. Yes, Mr. Chairman.

---

[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).

[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.

The CHAIRMAN. Dr. Albright, do you?

Mr. ALBRIGHT. No, sir. We covered it in the closed session.

The CHAIRMAN. Mr. McHale, thank you for being here. For the record, Mr. Stephen McHale is the Deputy Administrator, Transportation Security Administration. He is joined by Dr. Penrose Albright, Assistant Secretary for Plans, Programs, Budget, Science and Technology, of the Department of Homeland Security; and Ms. Cathleen Berrick is the Director of Homeland Security and Justice, U.S. General Accounting Office.

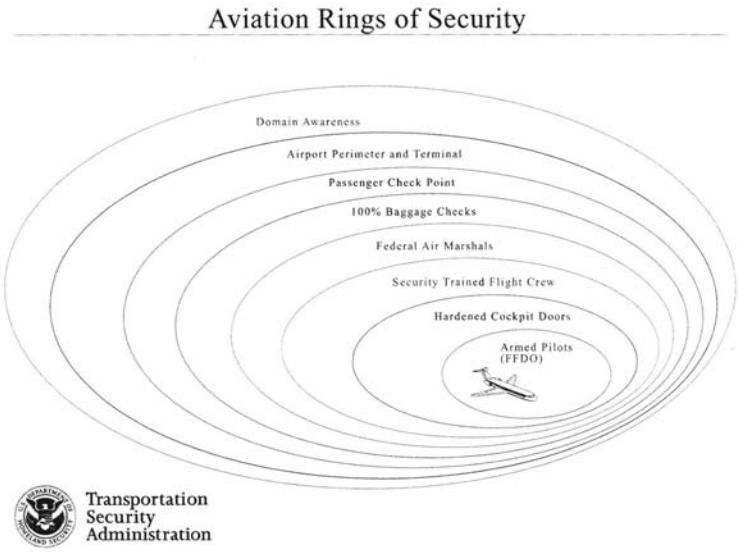
Mr. McHale.

STATEMENT OF STEPHEN MCHALE, DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION; ACCOMPANIED BY PENROSE A. ALBRIGHT, PH.D., ASSISTANT SECRETARY FOR PLANS, PROGRAMS, BUDGETS, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. MCHALE. Thank you, Mr. Chairman. Good morning, Mr. Chairman, members of the Committee. On behalf of Secretary Ridge and Administrator James Loy, I thank you for the opportunity to report on the Transportation Security Administration's progress in improving civil aviation security.

In the 20 months since its creation, TSA has made great strides in improving civil aviation security. I can tell you with confidence that the civil aviation security is more secure today than it has ever been. TSA has built a system of systems of security, illustrated on this chart to my right, that is based on multiple rings of security, from enhanced use of intelligence and better perimeter security, through passenger and baggage screening, the National Explosives Detection Canine Program, Federal air marshals, hardened cockpit doors, to armed pilots.

[The chart referred to follows:]



To achieve his objective, a terrorist must foil each and every obstacle we have laid in his path, and we continue to expand and strengthen each of these layers as we move forward.

TSA inherited a 30-year-old passenger screening system designed to detect obvious weapons such as guns, large hunting knives, grenades, etcetera. We have transformed that system with well-trained, highly motivated professionals who routinely detect much smaller and less obvious threats. We know the system is working better. Since February 2002, TSA has intercepted more than 1,500 firearms and more than 54,000 box cutters. We have reduced the list of prohibited items to exclude some commonplace innocuous items, yet the number of intercepted prohibited items continues to rise. Frankly, we are surprised that we continue to find such large numbers of items carried by travelers and we will continue to work on educating the public on the care they must take before heading to the airport to board a flight.

But it may be valuable, Mr. Chairman, to step back just a moment and look at what we have accomplished in a very short time. The poster on display tells a simple, factual, and I believe impressive story of then and now. For example, before 9/11 contract screeners had no national program of operating procedures or standards. Today Federal screeners meet consistent national protocols and receive much more robust and comprehensive training than their predecessors. Then, only 5 percent of bags were screened. Today 100 percent of bags are screened. Then, walk-through metal detector technology was outdated. Today we have state-of-the-art metal detectors at all airports.

[The poster referred to follows:]

Transportation Security Administration

Aviation Security System of Systems

THEN and NOW

Security Program Component	THEN (Pre 9/11)	NOW (After TSA)
Airport Security Screeners	Contract screeners with no national program of operating procedures or standards	Federal screeners operating in consistent, standardized security protocols who meet 100% of the national standards
FAMs	33 on International flights	Thousands on tens of thousands of monthly high-risk flights
Cockpit Doors	No hardened doors	All hardened doors
FFDOs	None	Hundreds now, more trained every week
Checked Baggage Screening	5% bags screened	100% of 1 billion bags screened annually
Federal Security Directors	None	158 FSDs for unified airport security
TIP	FAA 200 images	TSA 2,400 images
WTMD	Outdated technology	State of the art WTMD at all airports

However, no one element of our system of systems has a zero failure rate. As we have so often said, security is a filter, not a guarantee. That is why we have our rings of security. In case one layer is breached, the other layer will immediately be available to counter the threat. We must continue to evolve our system of people, technology, and intelligence so that we can always state with confidence that we are more secure than we were yesterday and that we will be even more secure tomorrow.

In order to know if we have actually improved security, we must be able to understand what our level of security is and how we are performing as an agency. To address this, we have implemented an aggressive program of testing and evaluation, and TSA will manage the overall risk of civil aviation security by focusing our efforts and resources on the highest threats. We continue to assess the relative risk of various elements of aviation in order to help us prioritize resources.

Let me be clear on one issue. We are well aware of our own system vulnerabilities and we take swift action to address them. For example, after the recent incident involving a TSA e-mail that had not been reviewed for 5 weeks, we implemented a series of steps to ensure that any potentially threatening e-mail sent to TSA is addressed immediately. Furthermore, last July TSA conducted a screener performance improvement study to determine the root causes of screener deficiencies and help us to prepare a plan to enhance screener performance.

Well before recent events involving smuggling of prohibited items on board aircraft, TSA began to make screening improvements ranging from more robust training to technology to increased management performance and accountability.

We continue to look for short-term improvements. Major elements of our short-term screening improvement plan are captured on this chart. Two important elements are recurrent screener training and supervisory training. All screeners must meet annual recertification standards and our first round of annual evaluation is under way. Most TSA screeners did not come onto the job until September and October of last year, so the annual recertification process began on October 1.

[The information referred to follows:]

Transportation Security Administration

Security Screeners
THEN and NOW

Issue	Screeners Then (Pre 9/11)	Screeners NOW (After TSA)
Employment	Contract employees	Federal employees
Selection Process	- Minimal Screening - No U.S. Citizenship requirement - Background Checks-minimal; no standards	- National comprehensive, competency based standards - Must be U.S. citizen or U.S. National - Extensive, customized and standardized background investigation
Pay	Minimum wage; no benefits	Improved pay and benefits
Training	12 hours classroom, 40 hours On the Job	40 hours classroom, 60 hours On the Job, end of training certification required
Certification	None	Annual certification required
Supervision	Through air carriers	Direct Supervisory Control
Attrition	100-400% annually	13.6% (2003)

We are implementing an enhanced version of the Threat Image Projection System, or TIP, to provide continuous on-the-job training and feedback. This is a system that superimposes threat images on X-ray screens during actual operations and records whether screeners identify the threat object. It is an excellent tool for evaluating the skills of each screener that enables us to identify screeners that require additional training or perhaps disciplinary action. Moreover, we can vary the images based on current intelligence so that our screeners are attentive to the latest threats.

[The information referred to follows:]

TSA SCREENER IMPROVEMENTS

Transportation Security Administration

SHORT-TERM SCREENING IMPROVEMENT PLAN

CATEGORY	ACTION ITEM
PEOPLE	1. Increase FSD Support and Accountability 2. Enhance Training for Screeners and Supervisors 3. Increase Frequency of Internal Affairs Covert Testing 4. Continue to Pursue Human Performance Improvements
TECHNOLOGY	5. Continue to Identify New Screening Technology 6. Complete 100% Threat Image Projection System (TIP) Deployment 7. Continue IT Connectivity to Checkpoints and Training Computers
PROCESS	8. Refresh Aviation Operations Policy, Procedures and Practice 9. Improve Workforce Management Scheduling and Staffing

The FAA installed TIP-ready machines that only had 200 images and that were not updated on a frequent basis. We now have considerably more images, well over 2,000, that we can update every day. We already have 1,450 TIP-ready X-ray machines in place and by the summer of 2004 all of our checkpoint X-ray machines will be equipped with TIP.

We also continue to research alternative technologies and seek short-term technology solutions to identify threats more accurately and quickly.

A very important element of this program and one I know is of great interest to this Committee is CAPPS, our automated risk assessment tool that we hope to have deployed early next year when we have satisfied you that we have addressed your concerns.

TSA now conducts covert testing in airports at over three times the annual rate of the old FAA red teams and we are increasing unannounced testing even further. Teams of engineers, trainers, and technology and management specialists work with Federal security directors to make improvements at airports that do not meet satisfactory performance levels and Federal security directors are held accountable for deficiencies.

This is an important point: We hold the FSD responsible for providing security at the airports in his charge and tie their performance evaluation directly to this requirement. But security is a partnership and we also hold air carriers and airports responsible for their contributions to security. To ensure that they are doing their part, we are hiring a cadre of new regulatory inspectors to monitor compliance with mandatory security requirements for aircraft, secure and sterile areas, perimeter security, and cargo.

With the holiday travel season only weeks away, TSA is concerned that with the increasing passenger flows we have been experiencing we could see longer lines this year than we saw last year at some airports. We often forget that travelers are also a partner in aviation security and they must do their part to prepare for takeoff. As we did last year during this time, we will be launching a large-scale public outreach effort so that we are not distracted at security checkpoints by false alarms or items that passengers merely packed by mistake. We want to be able to always focus our efforts on the real threat.

I can assure you that along with the air carriers and the airports and our many other partners, we have come a long way in answering the Nation's call to improve civil aviation security. But we must always remember that the threat the our security is constantly evolving and that we must ensure that we are always one step ahead of the terrorists.

Mr. Chairman, I thank you and the members of the Committee for your steadfast support of TSA as we strive to do our best for the American people, and I would be happy to answer any questions you may have.

[The prepared statement of Mr. McHale follows:]

PREPARED STATEMENT OF DR. PENROSE C. ALBRIGHT, ASSISTANT SECRETARY FOR PLANS, PROGRAMS, BUDGETS; SCIENCE AND TECHNOLOGY DIRECTORATE; STEPHEN J. MCHALE, DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION; AND WILLIAM H. PARRISH, ACTING ASSOCIATE SECRETARY, INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Good morning Mr. Chairman, Senator Hollings, and Members of the Committee. On behalf of Secretary Ridge, representatives of the Directorate of Information Analysis and Infrastructure Protection (IAIP), the Directorate of Science and Technology (S&T), and the Transportation Security Administration (TSA) are pleased to appear before you to discuss important improvements in civil aviation security. Our joint written statement will cover a wide variety of topics related to aviation security, and we are available to answer your questions in a closed and open forum.

Secretary Ridge and all of us at the Department of Homeland Security (DHS) appreciate the continued support that DHS has received from this Committee and the unwavering commitment of the Members to our mission to protect the homeland from terrorism, particularly our transportation systems and critical infrastructure. This is a vast undertaking that requires advancements in technology, improved intelligence, a dedicated workforce, a substantial financial commitment, the cooperation of industry and the American public, and hard work by all.

Understanding the Threat to Aviation Security

We believe that terrorists will continue to consider attacks against commercial aircraft in the United States and abroad likely intending to employ suicide hijackings and bombings as the most promising methods to destroy aircraft in flight, as well as to strike ground targets. Likely cognizant of changes in aviation security measures since September 11, 2001, they will seek out new ways to circumvent enhancements in aviation security screening and tightening immigration requirements. Additionally, the threat posed by terrorists equipped with man-portable air defense systems (MANPADS) is of credible concern. Indeed, the unsuccessful missile attack on an Israeli commercial airliner in Mombasa, Kenya, in November 2002 was a stark reminder of the threat posed by terrorists possessing MANPADS. MANPADS are widely available on black or gray markets around the world. Even an unsuccessful MANPADS attack on a commercial airliner would have a devastating economic and political impact. As you can well imagine, this is a serious and complex issue with no single solution. It is an issue of concern to the security of the homeland because MANPADS are relatively easy to operate and are small enough that they can be concealed in a vehicle.

- It's important to note that the U.S. intelligence community does not have any credible, specific intelligence information about planned MANPADS attacks against commercial aircraft in the United States. MANPADS generally do not pose a threat to commercial aircraft while flying at cruising altitude. They pose the greatest threat while aircraft are landing or taking off from airports.

Continually Striving for Excellence in Aviation Security

In the 20 months since its creation, TSA has made great strides in improving civil aviation security. TSA inherited a 30-year-old passenger-screening system designed to detect obvious weapons such as guns, hunting knives, and grenades, and has transformed it into a system that also finds much smaller but still dangerous items such as razor blades. This new system is working. Since February 2002, TSA has intercepted more than 1500 firearms and more than 54,000 box cutters. TSA screeners take pride in their work; this is not just a job but part of an important mission: to protect our Nation's transportation systems to ensure freedom of movement for people and commerce. However, recent events involving the smuggling of prohibited items aboard aircraft validate that our layered approach to security that cannot rely on any one system. TSA's layered system, including hardened cockpit doors, Federal Air Marshals, armed Federal Flight Deck Officers (FFDO), as well as passenger and baggage screening and the National Explosives Detection Canine Program, recognizes the fact that there is no such thing as a zero failure rate for passenger screening.

We are cognizant that there is much more to do. TSA has undertaken specific initiatives that will improve screening performance, and we are formulating a plan that ranges from more robust training to increased management performance and accountability to technological improvements. In addition, we have taken immediate steps to correct internal procedures at our customer response center to identify messages of interest from a security standpoint and ensure that appropriate action is taken swiftly.

TSA, working with the Department's S&T Directorate, will begin a comprehensive review of the civil aviation security system now that two years have passed since the enactment of the Aviation and Transportation Security Act and over twelve years have passed since the enactment of the Aviation Security Improvement Act of 1990. This is part of our constant evaluation of the security measures we have put into place, and now we have time to consider other approaches to aviation security that may be available to us.

Today, every passenger entering the sterile area of an airport is screened by members of a highly trained force of TSA screeners.[1] National, validated skill standards for all screeners form the foundation for an integrated system for hiring, training, certifying, and measuring performance. All screeners must demonstrate the qualifications, knowledge, skills, and aptitudes necessary to meet Federal standards and successfully perform as a transportation security screener. They receive a minimum of 40 hours of classroom instruction and 60 hours of on-the-job training. Screeners are subject to periodic proficiency assessments and unannounced performance testing. They are made aware of new threats and methods of concealment. This stands in marked contrast to the workforce responsible for U.S. airport security screening before the creation of TSA. Screeners employed by the airlines, often through contracts with private companies, received minimal training and were often poorly motivated. Contract screening forces were plagued with high rates of attrition that resulted in an average screener tenure of 4.5 months, making it all but impossible to develop and maintain the consistent level of proficiency required to ensure reliable screening.

Maintaining a high level of screener proficiency requires constant diligence. In July of this year, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, we gathered data from multiple sources to determine the actual, current level of performance and the root causes for the gap between desired and actual performance. Based upon this study, we have identified an array of solutions and are in the process of further evaluating and implementing them.

Two important elements of TSA's plan for screener improvement are recurrent screener training and supervisory training. Recurrent training is needed to maintain and enhance the skills of screeners, particularly in the areas of X-ray image interpretation, the search of persons, and the inspection of property. Supervisory training will enhance leadership skills in our workforce and provide the advanced technical skills needed to adequately supervise the screening process and resolve alarms.

Screeners who fail any operational test are removed from their screener duties and must complete remedial training prior to returning to duty. Remedial training includes an out brief by the Internal Affairs Agent conducting the testing and a review of all pertinent sections of the standard operating procedures (SOP) and Basic Screener Training modules. Our recurrent training program is under development, though two modules have already been delivered to the field. In the meantime, Federal Security Directors (FSDs) have been encouraged to use the training modules of the Basic Screener Course to address specific recurrent training needs. Many have done so, and others have developed their own supplementary training. Also, screeners are required to undergo weekly X-ray image interpretation training using state-of-the-art computer-based training. FSDs at airports have received the first of a series of screener performance improvement videos and more than 350 courses will be available via our new Online Learning Center or via will have access to compact discs. We are also certifying over 800 screeners and training coordinators to teach various topics at each airport.

Recently, approximately 500 of TSA's 3600 screener supervisors were enrolled in a U.S. Department of Agriculture (USDA) Graduate School Introduction to Supervision course through September. The course is being modified to specifically address airport security and will be introduced nationally this December. This course will be further tailored to meet the needs of screening supervisors, and we expect this enhanced course will be offered in March 2004. An advanced course is being developed for screener supervisors to provide them with a higher level of technical knowledge and skills.

All screeners must meet annual recertification standards, which require passenger screeners to pass an Image Certification Test, SOP Job Knowledge Test, and Practical Skills Demonstration, and require checked baggage screeners to pass an

[1] TSA is also operating a pilot program at five airports using private screeners that must meet all TSA eligibility, training, and performance requirements and receive pay and other benefits equal to those of TSA screeners.

SOP Job Knowledge Test and Practical Skills Demonstration. In addition to passing these tests, developed at the national level, FSDs will be responsible for ensuring that all screeners have a satisfactory record of performance in accordance with their individual performance management plan. Recertification for 2003–2004 began on October 1, 2003, and will run through approximately March 2004. As part of our recent rightsizing effort, approximately 28,000 screeners completed proficiency testing; we will consider successful completion of those tests to be a part of the annual recertification.

Another major initiative to improve screener performance is the implementation of an enhanced version of the Threat Image Projection System (TIP). TIP is a system that superimposes threat images on X-ray screens during actual operations and records whether or not screeners identify the threat object. This is an excellent tool for evaluating the skills of each individual screener so that we can focus directly on areas needing skill improvement. By frequently exposing screeners to images of a variety of dangerous objects, TIP provides continuous on-the-job training and immediate feedback and remediation. TIP allows supervisors to closely monitor screener performance and improvement.

TSA is expediting the replacement of approximately 1,800 conventional X-ray machines with TIP-ready X-ray machines (TRXs). We now have over 1,300 new TRXs in place.

Our TIP system is an improvement over the predecessor FAA system in several respects. The Federal Aviation Administration (FAA) created a library of only a few hundred images, which when shared with screeners, eliminated any real test value. In contrast, we are deploying a more comprehensive library of 2,400 images. We expect the new TSA TIP image library to be deployed on all TRX machines that are in place by the end of this calendar year. Through the combination of increased deployment of TRX machines and deployment of the expanded TIP image library, we will be able to collect and analyze significant amounts of performance data that had not been previously available to us. As we continue to deploy the expanded TIP library on all TRXs, we will primarily rely on using the limited library as an on-going training tool. Once TSA has the expanded TIP library on all TRXs in place, we will collect and analyze the data for December. The analysis will allow us to establish our first, national baseline view of screener performance, as measured by TIP, using the fully expanded TIP library of 2,400 images. This baseline view will help us better understand our strengths and weaknesses, allowing us to develop and implement appropriate skill enhancement strategies.

Of course, training alone is not sufficient to sustain excellence. To improve screener performance, TSA will increase unannounced, covert testing at airports across the Nation. Through covert testing, we challenge screeners to detect threat objects at screening checkpoints and in checked baggage, using simulated terrorist threat devices and current techniques. Timely feedback on the results of these tests is provided to screeners, FSDs, and other TSA officials to drive change and improvement through modification of our SOPs, remedial training, or improving technology, as appropriate. The covert tests serve as one of many indicators of screener performance. They must be viewed in the context of a larger performance measurement system that includes individual screener TIP data, annual screener certification, supervisory oversight, the adequacy of our SOPs, and the reliability of equipment and technology. Between September 2002 and October 2003 our Office of Internal Affairs and Program Review (OIAPR) conducted 847 checkpoint and 2,737 airport security access tests, as well as computer assisted passenger prescreening (CAPPS) and checked baggage tests at 107 airports. We are conducting covert testing at over three times the annual rate of the old FAA "red teams," and our testing uses more difficult, realistic testing situations. Although TSA cannot discuss the results of our tests in detail in this setting, results have shown an improvement of approximately 10 percent from September 2002 to August 2003. This is particularly significant because the difficulty of the tests has increased over the past year. OIAPR's testing plan is designed to test all of the airports during a three year period with Category X airports tested annually, Category I and II airports tested biannually, and contract screener pilot airports tested semiannually. Additional testing may be performed by each FSD.

As part of our continual efforts to improve screener performance, airports with below-par performance on covert tests will receive special attention. Teams of industrial engineers, trainers, performance consultants, and technology and management experts will identify the causes for poor performance at these airports and work with FSDs to design and implement solutions. Follow up will include additional covert testing and FSD accountability for any continued performance deficiency. We are also exploring ways to perform controlled studies to better understand team errors, communications, and interactions among screeners and supervisors with a goal of

improving the human capabilities that affect screener performance. TSA is making plans for delivering high-speed connectivity to all TSA locations within airports across the country. This will provide access to real-time training on current threats, connectivity with checked baggage areas, and will establish a foundation for planned implementations of additional administrative, surveillance, CAPPS II, and other security enhancements.

TSA works closely with S&T to develop and deploy technology that will help make our operations more effective, more efficient, less time consuming, and less costly. To help our screeners better identify explosives and weapons that an individual may attempt to carry into the cabin of an aircraft, we are testing two explosives trace detection portals that analyze the air for explosives as passengers pass through them. TSA has also established a new performance standard for walk through metal detectors (WTMD) and replaced every WTMD at all U.S. commercial airports with the latest technology. We are developing a document scanner that will detect traces of explosives on a boarding pass type document handled by a passenger. We are also evaluating "body scan" technologies, such as backscatter X-ray, millimeter wave energy analysis, and terahertz wave technology, but will not proceed with deployment on any of these technologies until sufficient safeguards are put in place to ensure the protection of passenger privacy.

We are continuing to work on identifying the next generation of explosives detection equipment for use in screening carry-on and checked baggage. We are working with the vendors of the currently deployed technology to develop enhancements to existing EDS platforms to improve alarm rates, throughput, and reliability. We are simultaneously working with new vendors to develop technologies that will enable us to detect explosives in smaller amounts than are currently established in our certification standard and will occupy a smaller footprint at already overcrowded airports. TSA is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat.

Although ATSA mandated the federalization of airport security screening, it held open the possibility that airports could return to contract screening, provided the high standards required of the Federal screening system could be met. TSA is currently operating a pilot program at five airports using private screeners that, by law, must meet all TSA eligibility, training, and performance requirements and receive pay and other benefits equal to those of TSA screeners. Beginning on November 19, 2004, any airport operator may apply to have screening performed by a contract screening company under contract with TSA. In preparation for this option, TSA recently awarded a contract to perform a rigorous comparison of the performance of pilot program screeners with that of Federal screeners, to determine the reasons for any differences, and to develop criteria for permitting airports to opt out of the Federal screening program. We will provide all relevant information to airport operators well before the November 19, 2004 date so that each airport operator can make an informed decision.

TSA is moving forward with the development of the second-generation Computer Assisted Passenger Prescreening System (CAPPS II), which will help us to focus our screening resources where they will be most effective. CAPPS II is yet another layer in our system of systems to address a continuum of security threats with minimal impact on airline customers and operations. CAPPS II is intended to identify terrorists and other high-risk individuals before they board commercial airplanes. CAPPS II will conduct a risk assessment of each passenger using national security information and information provided by passengers during the reservation process—including name, date of birth, home address and home phone number, and provide a "risk score" to TSA. The "risk score" includes an "authentication score" provided by running passenger name record (PNR) data against commercial databases to indicate a confidence level in each passenger's identity. CAPPS II will be a threat-based system under the direct control of the Federal Government and will represent a major improvement over the decentralized, airline-controlled system currently in place.

In developing CAPPS II, TSA is very mindful of the rights, liberties, and freedoms that define our Nation and differentiate our society from those who seek to harm us.

CAPPS II is being designed and will be built with the explicit requirement that privacy protection not become a cost of increased aviation security. CAPPS II is undergoing a rigorous course of testing and will not be implemented until it has successfully passed this test phase. TSA is cooperating fully with the U.S. General Accounting Office (GAO) so that GAO can issue the report called for in the Department of Homeland Security Appropriations Act, 2004, by February 15, 2004. Moreover, we are committed to continuous testing, evaluation and assessment of the system that is designed to ensure compliance with privacy policies—by our own experts, independent overseers, and the public. DHS is also contemplating creation of

an advisory council to review DHS programs, including CAPPS II. A Passenger Advocate will be available to work directly with individuals to help resolve problems caused by incorrect data. In addition, while we are developing CAPPS II and to ensure that concerns regarding CAPPS I are addressed, TSA has on-site customer support and supervisory personnel at U.S. airports to respond to any passenger concerns, as well as a toll-free call line and an Office of the Ombudsman at TSA headquarters.

CAPPS II would not retain data on U.S. passengers who are permitted to fly.[2] Information would be stored only for a sufficient time to assess that a U.S. traveler is who he or she claims to be and to evaluate Government information related to terrorist threats and practices. Information would not be kept after completion of the traveler's reserved itinerary, apart from a necessary audit trail that would not be searchable by passenger name or other personal identifier.

As part of its ongoing dialogue with the public on CAPPS II and related issues, DHS issued a revised Interim Final Privacy Notice, which provides information regarding CAPPS II, including the type of data that the system will review, and how the data will be used. The Notice requested public comment, and the closing date for submission of comments was September 30, 2003. We are now in the process of reviewing the many comments we received.

We are also developing the parameters for a pilot program to test key elements of the voluntary "Registered Traveler" program, including background checks, positive identification, and new checkpoint operations. We intend to test these concepts at several airports early next year. Our airline partners have expressed strong interest in working with us.

TSA has begun full-scale training of pilots who have volunteered for the FFDO program in close cooperation with organizations representing many airline pilots such as the Air Line Pilots Association (ALPA) and the Coalition of Airline Pilots Associations (CAPA). We have transferred FFDO training from the Federal Law Enforcement Training Center (FLETC) at Glynco, Georgia, to the new permanent site at FLETC's training facility in Artesia, New Mexico. The Artesia facility offers the capability to double student throughput each week, and we plan to do so in January 2004. FLETC Artesia is also the home of the basic training program of the FAMS, and thus, has training facilities specifically geared to the unique environment and circumstances present on an aircraft. TSA intends to use geographically dispersed facilities for semi-annual recertification training required of FFDOs, including private facilities. By the end of FY04, at the current pilot application rate, we expect to have trained the vast majority of pilots who have volunteered for the program and met the initial background requirements.

TSA has recently signed letters of intent (LOI) covering seven airports to enable them to efficiently integrate explosives detection systems with in-line baggage conveyor systems. The LOI, accompanying memorandum of agreement, and TSA-approved final system design plan collectively define the specific costs eligible for Federal Government reimbursement. Once the eligible reimbursement costs are identified, the Federal Government agrees to contribute 75 percent of those costs, while the airport invests the remaining 25 percent. We are continuing negotiations with additional airports to obtain a LOI where this makes practical and economic sense. For those airports that will not be covered by an LOI, we continue to work on screening solutions that can accommodate 100 percent electronic screening of checked baggage for explosives.

Cargo security on passenger aircraft is a concern for all of us engaged in transportation security. Proposals to require the physical inspection of every piece of cargo shipped on passenger aircraft without a risk-based targeting strategy are no more practical than similar calls to physically inspect each of the more than 6 million containers that enter the United States each year through our seaports. Proposals of this sort would simply prevent cargo from being carried on-board passenger aircraft. Rather, TSA has focused its efforts on three key components in ensuring the security of air cargo. First, cargo deemed suspicious or "high-risk" will be subjected to more intense security screening under the TSA approach. Part of this process involves banning cargo from unknown shippers from passenger aircraft, and greatly strengthening the "Known Shipper" program. Passenger air carriers, all-cargo carriers, and freight forwarders have been given added responsibility for verifying a customer's status in the Known Shipper Program. TSA performs inspections of these links in the supply chain to ensure compliance. TSA is also moving forward with the Known Shipper Database and automated Indirect Air Carrier certification/recertification. TSA plans on the full deployment of this database in FY 04. TSA is al-

[2] Data on non-U.S. citizens may be retained longer to facilitate identity authentication if adequate public records used by the CAPPS II system do not exist.

ready working with the Bureau of Customs and Border Protection (BCBP) and its National Targeting Center in the development of tools for pre-screening air cargo to determine which of it is truly high-risk. Finally, TSA will need a toolbox of inspection methodologies and technologies for inspecting high-risk cargo, as no one technology or technique can be applied in all operating environments. A combination of inspection protocols, and EDS, ETD, X-ray devices, canine explosives detection teams, or perhaps even emerging technologies will need to be made available to the field.

TSA is grateful for the cooperation that we have received from the industry through its participation in cargo working groups, an offshoot of the Aviation Security Advisory Committee (ASAC).[3] On October 1, we received 44 recommendations from these groups, covering twenty-two topic areas, including enhancements to Known Shipper program, the development of additional screening technologies, greater security of Indirect Air carriers (freight forwarders), and enhanced security measures for the all-cargo air carriers. TSA is reviewing these recommendations as part of the development of a strengthened regulatory program and the completion of the agency's strategic plan for air cargo.

Our continuing efforts to improve aviation security inevitably focus on more accurate information about people who have access to various aspects of the aviation and overall transportation system. Through our Transportation Worker Identification Credential (TWIC) program, TSA is developing a uniform credentialing standard that has the potential, if necessary, to be used across transportation modes for personnel requiring unescorted physical and/or logical access to secure areas of the transportation system. Uniform credentialing standards will enhance security and make economic sense to an industry for which multiple cards and mixed standards are commonplace. On October 21st TSA concluded a technology evaluation in two regions. One was on the East Coast covering the Philadelphia-Delaware River area, and the other was on the West Coast in the Los Angeles and Long Beach area of California. The information that we glean from these technology evaluations will enable us to make key decisions about further development of this program.

TSA is focused on four key areas and related technology projects to enhance airport perimeter security: (1) security of access control through intended entry points; (2) security surveillance of perimeter areas; (3) improved security response capability to intrusions and security breaches through automated decision aids; and (4) oversight of industry compliance with current security requirements. TSA has collected and catalogued information on more than 300 applicable security technologies that include: biometrics, detection and prevention devices, surveillance technologies, and proximity sensors. Testing and evaluation of these and other technologies will be performed by TSA in partnership with airport operators who have volunteered to be participants in the 20 Airport Access Control Pilot Program. TSA hopes to select the first 5 airports and technology plans by the end of 2003. TSA also has the ability to test and evaluate these types of technologies in conjunction with the activities of the National Safe Skies Alliance at airports throughout the country

The realization of and the response to the threat from Man Portable Air Defense Systems (MANPADS) are part of our focus on perimeter security, an element of the security plan required for each airport. With the Directorate of Science and Technology (S&T) of DHS and the Department of Defense, TSA is undertaking efforts to come to a cost-effective, scientifically practical solution to the threat posed by MANPADS. Protecting civil aviation from MANPADS remains a multi-faceted undertaking—research into technical countermeasures is just one facet. Other components include enhanced security beyond the airport perimeter, non-proliferation efforts, and border and customs enforcement, all key areas that DHS, the State Department, the Defense Department, and many other agencies continue to pursue.

The Contribution and Potential of Technology to Improve Aviation Security

The Department of Homeland Security's S&T Directorate is conducting a competitive, multiple phase effort to develop countermeasures to shoulder-launched missiles that may be employed by hostile forces and terrorist groups against commercial aircraft. This S&T program, referred to as Counter-MAN Portable Air Defense Systems (MANPADS), was initiated in 2003 to identify existing candidate technologies that could lead to an effective and affordable solution for commercial aircraft. Clearly, any acquisition plan for such countermeasures must include a cost-benefit analysis that addresses the full range of relevant issues, including efficacy, cost-effectiveness, training, and not least of all, countervailing safety considerations. Proactive discussions of all of these issues are currently ongoing between DHS, other affected agencies and private industry.

Military missile countermeasures, such as the Large Aircraft InfraRed Counter-Measure (LAIRCM) unit using Directed InfraRed CounterMeasure (DIRCM) techniques exist in various stages of development and deployment, but are generally restricted to military and Heads-of-State aircraft. The defense industry has also performed limited evaluation of tower-mounted IRCM subsystems for ground-based applications as an alternative to airborne installation.

Primary challenges to commercializing military IRCM equipment for application to civilian aircraft include: affordability in total cost of ownership; vastly improved reliability over their military counterparts; less labor and time-intensive maintenance interventions; lower false alarm rates; and countermeasures that are safely applied in operating environments of civilian aircraft. IRCM commercialization will require tightly integrated systems engineering, development, test and evaluation of existing and emerging military Aircraft Survivability Equipment (ASE) for suitable equipment and processes that can be redesigned to protect civilian aircraft.

An Industry Day was held on 15 October 2003 in Washington, DC to describe the Counter-MANPADS Program procurement process, which began with an invitation for industry to submit White Papers and Corporate Qualifications. The conference, hosted by DHS S&T, was attended by over 200 participants from 91 organizations. To hasten program commencement, DHS S&T will utilize the procurement instrument known as Type 845, Other Transaction Agreements.

Twenty-four white papers were received from industry on October 27. Invitations for full proposals will follow to those respondents with the most promising white papers. At least two awards are projected during the first phase of this program, which begin in January, 2004. A second program phase will result in a down-selection of the one or two most promising design candidates, and prototypes will be tested in simulated and live-fire environments.

An important consideration in the selection and deployment of IRCMs aboard DOD Civil Reserve Air Fleet (CRAF) aircraft is the use of countermeasures in civilian airspace—specifically, in populated areas. In the event of a MANPADS launch, traditional military pyrotechnic countermeasures (flares) often represent a major safety hazard to property and personnel. Directed countermeasures, such as an onboard laser to disrupt the MANPADS sensor and steer the missile away from the aircraft appear to be the most promising ASE candidates for application to civilian aircraft.

In conclusion, since the tragic events of 9/11, and we have come a long way in answering the Nation's call to improve the civil aviation security system. We better understand the threats to security and have dramatically improved our capability to share information on threats. We have built a highly skilled and professional screening force and have worked diligently to assure that imbalances in the initial placement of screeners in airports across the Nation are corrected by staffing adjustments. We have enhanced security technology at airports across the Nation and are exploring potential solutions for new threats, including those posed by MANPADS. We are well on our way toward implementation of a CAPPS II system that will greatly enhance our ability to keep terrorists off of commercial airlines, without disturbing the efficient flow of passengers or compromising their privacy. We have all learned a great deal very quickly, and will continue to do so, always striving to use every tool at our disposal to drive toward excellence.

The CHAIRMAN. Thank you very much.

Mr. McHale, I was not surprised that TSA has experienced significant difficulties. This was a huge, massive formation of a Federal workforce with significant responsibilities and training requirements. What I am concerned about concerns Ms. Berrick's testimony and what I have been told is a lack of measures of TSA's screening effectiveness. I do not know how we make progress or can know what areas need to be improved unless we have some measures of determining what progress or lack of progress is being made, where our failings are.

Mr. MCHALE. Mr. Chairman, the first year, really 14 months, of TSA where we were primarily focused in our measurements was how we were doing in standing up the agency and how we were doing in getting out there to the airports. Having done that, we are now very much focused on measuring our performance and moving forward with that.

We have actually worked with GAO to identify ways that we should measure that. The TIP system that I mentioned has built into it the ability to measure when a screener identifies or does not identify a threat image. That gives us very real screener by screener feedback on how they are doing on the X-ray system.

We also, through our covert testing system, we are trying to observe how the screeners actually perform their standard operating procedure on the wanding of passengers, etcetera. We do have systems in place that work very effectively in testing the explosive detection systems, some of those which are wired in.

It is an ongoing issue for us. We did not inherit a system in which checkpoints were connected into the computer systems, where we could download that kind of data. We are working all the 1700 checkpoints in the country over the next couple of years to try to get that connectivity in, to give us that sort of data. It is a very important issue for me. It is something that obviously I look at every day.

We have I think a very good backbone called the "Performance Management Information System" for gathering that data, and every day we are getting more data. We do not have enough.

The CHAIRMAN. Ms. Berrick.

Ms. BERRICK. I think the most important step that you have to take in measuring performance is first establish a plan on how you are going to do that and specifically identify the data that you need to collect and what you are going to measure. TSA was mandated by the Aviation and Transportation Security Act to develop a short-term annual performance plan and they did do that. However, that plan was primarily focused on meeting the actual mandates: how many screeners do we have in place, how are we doing in terms of checked baggage screening. It was not really based on how effective they were on those two functions.

TSA is developing a 5-year annual performance plan, as required by the act, that they are focusing on providing more performance measures that are outcome versus output measures, so they will be measuring effectiveness. An example would be their covert testing program. Instead of saying, we need to conduct a thousand covert tests during the year, the measure would be we need to achieve a pass rate of X percentage related to this covert test. I think that is the most important step in establishing performance measures.

Related to the passenger screening program, I think fully implementing TIP should be a high priority, which I know it is, within TSA. I think also the Performance Management Information System that Mr. McHale mentioned should be expanded to collect additional performance data. Right now it collects little performance data related to passenger screening. It does collect some other types of data. I think that should be expanded. The annual screener certification program is another source of data that should be rolled out.

So I think that TSA is moving in the right direction, but I think the first step is establishing a plan on how they expect to achieve this.

The CHAIRMAN. Well, I hope we can get that soon, Mr. McHale.

Dr. Albright, at the first hearing we had with Admiral Loy we talked about technology. I do not believe that the airline industry

is going to return to its fullest capability until Americans who want to fly on an airliner have some kind of confidence that they will be able to move through the security screening process with some degree of predictability and dignity.

I go to the airport at least every Friday and every Monday, either National or Phoenix Sky Harbor. Some days I go and you go right through security. Some days I arrive and the line is all the way out the door and then we experience the panic of thinking that I am going to miss the flight even though I am there the required amount of time.

I want to know what your assessment is. What is the state of this technology that is going to both preserve security, which we all admit is the first priority, but at the same time restore some kind of normalcy, stability, and predictability to the screening process, which can only in my view be achieved by technological advances.

Mr. ALBRIGHT. Let me answer that in a couple of ways. First let me say that it is my view that TSA has in fact deployed the state-of-the-art.

The CHAIRMAN. I do not disagree with that.

Mr. ALBRIGHT. But having said that, I think it is also important to note that, and it has been a common thread in the answer to the prior question, I believe, that what happened was about 2 years ago in a fairly ambitious and rapid effort we deployed technologies as quickly as we could to protect the American public.

I think what is probably important to do now—and I will say that both Secretary Ridge and Admiral Loy have asked the Science and Technology Directorate to do this—is to now step back a bit and look at this problem from a more fundamental system engineering point of view and ask some basic questions: Do we have in fact the appropriate technologies, as you are pointing out, and the appropriate kinds of performance that we need to have at passenger screening checkpoints? Are they deployed in a way that is not just intended to make us secure, but also intended to be efficient as well?

Of course, the same holds true for luggage screening and for cargo screening. So we are initiating this study at the request, again, of Admiral Loy and Secretary Ridge, working closely with TSA to do a full end-to-end systems engineering study of the aviation security environment and ask the question basically, can we make this more efficient, can we make it more repeatable than it is today.

The CHAIRMAN. Well, my time has expired, but I wonder if there is not some—hopefully, there is some technology in the works that would improve this situation, both from the passenger standpoint as well as the baggage standpoint.

Senator Boxer—oh, Senator Lautenberg. Senator Lautenberg. I am sorry.

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. I wanted to talk about the air marshal program and ask a simple question: Are we continuing to train air marshals and have the numbers of air marshals—I do not want to

go into too sensitive an area, but people know that we have them and do we have more than we had before? They are doing a good job and we need them, but we heard testimony in private that, without revealing anything, that said that they are an effective part of our security system.

Who can tell me?

Mr. MCHALE. We are training new air marshals, Senator, and they are an effective part of the system, within our entire system of systems. We have, as we have said publicly, thousands more than we had pre-9/11, and we think that the numbers are about right, although one of the issues behind—one of the reasons behind the movement that you referred to in the closed session, the movement to the Bureau of Immigration and Customs Enforcement, is in fact to cross-train some of the Customs and Border Patrol agents to be available in the event of need for surge, as you know.

Also, as you know, law enforcement agents, many of the officers, many of them are allowed to fly armed if they are on official business in the United States. We are also looking for ways to capture that information ahead of time, knowing when they will fly, so that we can use them to bolster our force of people who are on aircraft who are able to defend the aircraft.

Senator LAUTENBERG. This to me sounds a little bit like boxing and wrestling. They are both contestants, but they have different skills. And I am afraid of kind of watering down the possibility that those who are skilled at working in the airplane cabin and those who are working along the deserts and so forth—the chairman knows about those kinds of guards that we need. They are quite different assignments.

I want to get into something else, because to me this is a golden opportunity to talk about another issue. With all the focus on baggage screeners and all of the training that we want to give and the measurements that we want to develop, this now has become an integral part of our security operation. I do not understand why in the world that it is possible that we want to go private with the FAA when we have now, we have had a discussion, without revealing any secrets, about the availability of small weapons that can take down airliners—SAM's, you name it, other kinds, RPG's.

The fact of the matter is that here we have an organization that works effectively. I consider that the FAA is the fifth branch of the military. It is 24/7 and do whatever you can. And whether it was in reaction to the World Trade Center attack and bringing down 5,000 airplanes safely to destinations that were not originally planned, and making sure that when the Challenger fell out of the sky that they moved the aircraft around, it is the strongest measure of safety that we could have.

I do not believe that it makes sense to be so focused on baggage screeners while we dismiss the possibility that the FAA should stay within government hands. I think it is an outrage to propose. It is not a question, Mr. Chairman, but it is a statement, when I see how focused we are, properly so, on effective baggage screening and here on airplane screening, and we are all worried about how we protect airplanes when we know that there is a threat out there that a missile or a weapon could be fired at an airplane, and not to have the same skills, to have Acme Air Service taking care of

our flight control, I do not think makes sense in any way. It is an issue, Mr. Chairman, that I intend to focus on with all of my energy.

But we have succeeded in having a very good hearing with excellent witnesses. Ms. Berrick, we wish you confirmation, good luck, and all that to all of you. We thank you for your service to your country.

Ms. BERRICK. Thank you.

Mr. MCHALE. Thank you, Senator.

The CHAIRMAN. Senator Snowe.

STATEMENT OF HON. OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman.

I wanted to raise several issues today. Obviously, we are all familiar with the incidents that occurred with the box cutters and that also occurred on a plane that left an airport in Maine and went to Boston and they discovered, the maintenance crew discovered, box cutters on that plane as well.

I think the real question is whether or not these are isolated, random incidents or is it part of a troubling pattern, and second whether it is a screening problem or a training problem. Now, we have heard both, and I would like to have you address that, Mr. McHale, because I think ultimately—I know that we have come a long way with respect to aviation security over the last 2 years, and obviously for billions of dollars. So it is the linchpin of our homeland security without question.

I think the real issue is that if these incidents keep occurring, it only takes one incident to create a catastrophe, as we well know. I think the question is why these are occurring, is it the screening or is it the training? Now, I know the company that has manufactured these screening machines at the airport claims it is the training procedures that are deficient in identifying these types of weapons.

So I would appreciate your response and what you have done in the meantime. I understand that in your testimony earlier—I am sorry I missed that part of it; I had to leave for a minute—that—do you have safeguards in place to identify e-mails?

Mr. MCHALE. Yes, we do, Senator.

Senator SNOWE. What happened in this instance that you failed to respond for, what was it, 5 weeks?

Mr. MCHALE. 5 weeks. We have put those safeguards in place since that incident. What we have done—the e-mail came in to a consumer response center, one that we had only recently started up and that was receiving a very large volume of e-mails. What we realized is that—and probably should have realized earlier, but what we recognized was that this was a potential place where someone could send in a threat or a threatening e-mail.

What we have done is established, first of all, an automated screening system that pushes these e-mails into a special place where we can review them. Second, we have trained everyone who receives these types of e-mails on what to look for and what to do with them. And then we have procedures for the referral of it to the appropriate security personnel who can respond.

So we are pretty confident in the system we have got in place. We review that four times a day, including in the middle of the night, partly because some of the areas we serve are around the world and e-mails can arrive in the middle of the night. So we look at that all the time, trying to sort through that and identify the threats.

On the box cutters generally, I think there is a number of important things or issues there. One is that we do not regard security as any one thing. It is not about equipment, it is not about training, it is not about people. It is about all those things. It is not about the screening checkpoints, but it is also about perimeter security, it is also about the maintenance workers and others. We have to look at the entire area for what the vulnerabilities are.

We believe that there may be a little bit of testing of the system going on, which may be why we are seeing a little more activity in that area. Historically, we have found box cutters left on planes by maintenance workers. That is something we are working with the airlines to tighten up on and make them aware. They are being very helpful in that regard.

But I think that it is important also to recognize that, at least in some areas, while we have, as Assistant Secretary Albright said, we have state-of-the-art technology, we need better technology. The screening system pre-9/11 detected guns and grenades and large knives. We have improved a lot of that equipment. We have improved our training, and we pick up a lot of smaller items. But as you get to smaller items, smaller and smaller items, it gets harder and harder and more difficult to see it in the X-ray machines or even with the metal detector technology.

So we try to adjust all—try to look at all of those things together and do the best we can. But part of this is going to be better technology, 3D X-rays and other things that we are working with the Department to get out there and deploy, working with industry to see what ideas they have. We will get better, but it continues to be a challenge.

Senator SNOWE. Well, as I understand it, according at least to an article that was printed recently, that there is a divergence of opinion about what is the issue, in terms of whether it is training or the X-ray machines. The company that manufactures these X-ray machines claims they can be detected.

So I think the bottom line is here, is that it is obviously important to reconcile that difference and address it, whatever it is.

Mr. MCHALE. Right.

Senator SNOWE. It undermines confidence, in the final analysis. As I think as we all know, it only takes a few incidents like this to undermine the public's confidence about the procedures in aviation security.

Mr. MCHALE. I could not agree with you more. I think, though, it is a mistake to focus on, try to focus on one thing or the other. Machines certainly can detect the equipment in a controlled setting, but in an operational environment you need to look at the machine, you need to look at the way the bags are packed, how they are moving, how fast they are moving, the training of the screeners.

You need to look at all of it, the environment, the supervision. You have to look at the whole system in an operating environment, and that is what we study every day, trying to figure out how we can improve that.

Senator SNOWE. Yes, I have no doubt, and I understand what you are saying in terms of the volumes and so on. It is good to look at the entire picture.

Ms. BERRICK. Senator, can I make one comment about training?

Senator SNOWE. Yes.

Ms. BERRICK. Related to the passenger screening program, we recently did some work where we looked at training for passenger screeners, and we identified some good aspects of the program and some aspects that need to be improved. TSA did develop a basic screener training program and a remedial screener training program. When a screener fails a test they have to go through the remedial training.

In fact, their basic screener training program is more than what was required under FAA. However, we did find some weaknesses in terms of recurrent training, having training on a periodic basis to reinforce skills and update skills, and also supervisory training. TSA is taking some efforts to strengthen their recurrent and supervisory training programs, and we are going to continue to look at that.

Regarding the Threat Image Projection system, which TSA is fully implementing, that is also a good training tool in addition to testing. But there is other training I think that needs to be implemented in terms of how to manually search a bag, in addition to just recognizing the images on the screen, and that is something that we are continuing to look at.

Senator SNOWE. I appreciate that.

Thank you.

The CHAIRMAN. Senator Boxer.

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Thank you very much.

Picking up on Senator Snowe, each layer—I understand we have a layered defense, but each layer has to be as good as it can be. You are totally right, Mr. McHale. It is not one thing. It is not one thing, but it is everything, and each layer has to be as good as it can be, obviously.

First, I want to thank my Chairman, because this has been a very important morning for me. The session we had before, going into some of my concerns, I just appreciate the opportunity, Mr. Chairman. And I know you have made that commitment to me and you kept it. I thank you.

I want to say to our witnesses from Homeland Defense that you have a huge job. You know that. We appreciate it. It is quite a task to take an industry—and I think Senator Lautenberg pointed out—that was made more accessible to people as the years went on and now try to weed out bad apples. This is not easy. So I want you to know in that context, if I am tough in my questioning, I understand the challenge you face.

I also am not one who believes that funds resolve everything, because if you do not know what you are doing you are going to misspend a dollar or ten. But I think GAO has pointed out there are some challenges regarding resources, and I think—and I just hope—I am not asking you to comment today—that you will let the Chairman know and others know if we need to have more of a priority here, because I have some concerns about it.

I want to start off with the shoulder-fired missiles. I sound like such a broken record, I apologize. But I am going to just keep on this until we are doing this thing and we have got a plan and it is going to happen. Have you seen the CRS, either of you, the CRS report of September?

Mr. MCHALE. Yes.

Mr. ALBRIGHT. Yes.

Senator BOXER. OK. I am just going to highlight this for the public, a few things they pointed out. There are 700,000 shoulder-fired missiles that have been produced worldwide in a number of countries—one, two, three—12 countries. There are 27 militia groups and terrorist groups estimated to have these 700,000, at least some of these 700,000, not all of them, missiles. These missiles are cheap, easy to conceal, easy to use, and effective, according to CRS.

Other important points. The FBI estimates airliners hit at least 29 times over the years, causing 550 deaths. Rand says as many as 40 civil aircraft were shot down between 1975 and 1992, causing up to 760 deaths. The CIA reports in 1997, 400 casualties up to that point, 27 incidents. We have various estimates because sometimes they are not positive on this, but this is what, this is the range.

What I fear is that, because of circumstances now as they are in Iraq and in Afghanistan, which Afghanistan I think is going much better, I am worried about more access to these missiles and I am worried about this being something we are going to have to be very concerned about. Needless to say, we saw what happened with the helicopter in Iraq. Our beautiful young people coming home, trying to get home for R and R, were met with this fate, too many of them, 16 I believe, and many injured.

So it is hard to find the people who did it and it is a very big challenge for us.

Have you discussed air traffic control options?

Mr. MCHALE. Yes, Senator.

Senator BOXER. OK, because that is something that they recommend we look at in terms of how do you evade and not be so predictable.

Mr. MCHALE. Yes.

Senator BOXER. So I think it would be good if we did some of that. But we ought to let that out, that we are taking some—we do not tell them what it is, but we are doing things a little differently. It would throw somebody a little bit off.

How about airport and local security? You are making these threat assessments. I have mentioned many times about my San Diego airport. The chairman has pointed out, well, in San Diego someone could just be in an office building. That is all true. You cannot do the impossible. But in my view, when I am standing like

on top of the roof of the garage—the airport people said, we never really thought about this. They said they were going to take action.

How many of these threat assessments have you made on the major airports?

Mr. MCHALE. We have done all of the 20 largest airports in the United States, the 21 largest airports in the United States. We have done—we have done a lot more. I am just trying to think of—I do not want to go too far into that.

Senator BOXER. Are you instituting changes, working with those airports on some of the security measures?

Mr. MCHALE. Yes. We have worked with the airports and, perhaps just as importantly, we have worked with local law enforcement. This is not a threat people thought about a long time ago.

Senator BOXER. Of course not.

Mr. MCHALE. So there is a lot of education that has to go on about what to look for, what the vulnerabilities are, etcetera. So we are really engaged in a very big education effort at the local, state and local law enforcement level about what the vulnerabilities are and how they can work together with us to improve the perimeter.

Senator BOXER. Well, I can assure you my airport people want to help.

Senator Stevens mentioned working with the communities on civil defense, because these perimeters are so large. Have you looked into that?

Mr. MCHALE. We have worked—we have worked with actually some of the local industries and companies around airports that control a lot of the private land and the security forces. Many airports tend to be more in industrial areas. I think that is probably what I want to say about that.

Senator BOXER. Well, perhaps maybe we could be briefed privately on this——

Mr. MCHALE. I would be happy to do that.

Senator BOXER.—because I just think if citizens want to help this could be a really interesting and important way for them to help around the perimeters.

I see that the red light is on, so I will withhold.

The CHAIRMAN. Please continue, Senator Boxer. I know how important this issue is to you. Please continue.

Senator BOXER. Thank you. Thank you very much.

I just want to say this. I do not expect any answer from you because this is really kind of a fight in the Senate family, which is about the future of air traffic control, and Senator Lautenberg mentioned it. I just feel like we need to consider above all the safety of our people. I know that we have this FAA bill. I very much want to see it come forward and very much support everything in it.

I think we should have done more to stop the privatization of the air traffic control jobs, because I think Senator Lautenberg makes a point: We are focused on screening and all the other things, and they are so important, but if we do not have people who are thoroughly trained, especially since we may, according to your own answer to me, be instituting new ways of bringing planes in, new and different ways—I think it is important to note that the idea of privatization was so frightening to a Congressman over on the other

side that he put in the FAA bill that it could never ever happen in his State, and all the other states could be affected by an Executive Order.

So I do not want to put you on any type of a spot, but I know if you ever have the opportunity to think this through, if you have opinions, sharing it with our President would be great.

I have other questions. I will wait for another round, on different subjects.

The CHAIRMAN. Senator Snowe. Senator Snowe, do you have any?

Senator SNOWE. Yes, I just have a couple more questions, Mr. Chairman.

One is on air cargo. I would just like to understand where TSA is at this point in time and how effective the Federal Known Shipper Program is. As I understand it, in the appropriations for next year there is language, the Secretary of Homeland Security is directed to research and develop certified systems at the earliest date possible. So when will TSA be ready to do this?

This is obviously one of the gaping holes in the system. I think that everybody has acknowledged that. I think the General Accounting Office has acknowledged that. This is something that has to be addressed sooner rather than later.

MassPort Authority as I understand has created a pilot program. So I think obviously some of the airports are going to be taking this initiative and that is a good thing, but obviously we need a national system as well. I mean, when less than 5 percent of all air cargo is being screened that is disconcerting, to say the least.

Mr. MCHALE. We have actually—I met with the Administrator of MassPort a couple weeks ago to talk partly about this and what they are doing. We have also talked with the Israelis, with a number of other countries that are interested in cargo security. Again, the challenge is the technology. X-ray machines only tell you so much and they do not necessarily in a large cargo container help you with the detection of explosives and things like that, and the larger equipment that helps with that is very slow.

So this is an R and D problem and we are very glad that the Administration has provided us with quite a bit of funding in that area. We are also going to work with the Department very closely to do the research here, but we do need some—we do need some better technology than we have today to deal with this.

What we are going to do in the mean time as we are going down that is really try very hard to identify the high-risk cargo. This is something that we have done internationally for a number of years. We are going to bring that, bring that over domestically so that we can inspect, physically inspect, 100 percent of high-risk cargo going onto all cargo aircraft.

We are trying to very much enhance our Known Shipper Program. We just completed a round of work with the Aviation Security Advisory Committee where they made a number of recommendations to us—that Committee is made up, not only of industry members, but also consumer groups, passenger groups, and others, victims groups—where they made a number of recommendations about how to further secure the system, both look-

ing into the future but also in the short term with what we have got.

We will have—we are increasing our use of canines, which is perhaps the best technology we have got out there in many ways today. We are using that extensively with the Postal Service and we are just starting a testing program really to see how we can use that in the operational cargo environment.

So we have got a lot of different initiatives going on. I think the first one that is going to bear fruit is going to be the improvements to the Known Shipper Program.

Mr. ALBRIGHT. Senator, if I could add to that. To do much beyond what Mr. McHale has just pointed out is going to require some significant re-engineering of how we actually deal with cargo coming into airports. Clearly the best approach is to do it while it is still break-bulk and prior to its assemblage into a pallet or into a cargo container. Different technologies—and in order to do that would require a significant change in the way these freight assemblers who are located at airports actually do business.

The second issue is, or the second point to make, is that the technologies you use for different sorts of cargo are very different. X-ray technology may work perfectly fine if you are looking at a cargo that is clothing, for example. It will not work very well at all if you are looking at automotive or electronic parts. So you would need a spectrum of technologies and some way of separating out the different sorts of cargo prior to the inspection process to, again, to significantly change or increase the amount of cargo inspections other than what Mr. McHale pointed out.

Senator SNOWE. Did you want to say something, Ms. Berrick?

Ms. BERRICK. Sure, I will just make a comment. GAO has done some work in the past looking at the security of air cargo and we did make specific recommendations to strengthen the Known Shipper Program, some of which I know TSA has implemented. For example, one vulnerability that we identified was the security at transfer points where the cargo is collected before it is transported to an aircraft and loaded onto an aircraft. So we believe that strengthening, continuing to strengthen, Known Shipper Program is important, as well as increasing inspections of targeted cargo, as well as focusing on R and D, which I believe $55 million is appropriated for for 2004.

Senator SNOWE. One final question concerning carry-on explosives. I know the Washington Post published an article on the 14th of October outlining the Department of Homeland Security's concern about Al-Qaida attempting to create a chemical called nitrocellulose. What steps is TSA taking to address this threat, because obviously we do not have the capabilities at this point to identify plastic explosives?

Mr. MCHALE. We do have those capabilities, actually, if we do a trace detection——

Senator SNOWE. How prevalent?

Mr. MCHALE. If we do trace detection on the item, we could discover nitrocellulose.

What we are doing obviously is looking—I think the *Washington Post* reported a teddy bear or some soft pillow stuffed with nitrocellulose. That alone does not make an effective explosive, so there

has to be additional things there, and those are things that we can look for and do look for.

We have trained—we have gone out and informed the screeners—we actually send them a daily update on new threats and how to look for them and discover them. So we have done some training in that area to try to identify the things that they have to look for and see.

Senator SNOWE. I see. But plastic explosives could be readily identifiable and detected?

Mr. MCHALE. They are best detected by explosive detection technology. We do not have—and the best things to do that are the large baggage kind of machines that we use. We do not have those at checkpoints, mostly for reasons of space actually.

Senator SNOWE. Yes, where the checked baggage is——

Mr. MCHALE. Checked baggage, they will find it.

Senator SNOWE. But the baggage, though, accompanying the passenger going onto the plane is another issue, is that correct?

Mr. MCHALE. The carry-on bag does not typically go through the large EDS machines, unless we have a reason, some reason to suspect, in which case we will send it back, send it back down and run it through one of the big machines.

Senator SNOWE. But so at that point it could not be detected; is that what you are saying?

Mr. MCHALE. The X-ray machines could detect some of the items that would be, some of the additional items that would be needed to actually ignite the nitrocellulose and turn it into a bomb.

Senator SNOWE. Thank you.

The CHAIRMAN. Senator Boxer.

Senator BOXER. Thank you, Mr. Chairman.

Have you looked at blast-proof cargo containers made of Kevlar?

Mr. MCHALE. Yes.

Mr. ALBRIGHT. The answer is yes.

Senator BOXER. What do you think?

Mr. ALBRIGHT. The issues in the past—well, firstly, as you know, the cargo containers are really only relevant for wide-body aircraft. We typically do not put into containers cargo that is on narrow-body aircraft.

Generally the issues associated——

Senator BOXER. But commercial aircraft carry cargo.

Mr. ALBRIGHT. They carry cargo, but generally the large containers that you are referring to are generally used on wide-body aircraft.

The CHAIRMAN. Yes, so go ahead. What do you know about this?

Mr. ALBRIGHT. In general what has been found—and Steve, you can kick in here—is that there is actually a fairly enormous—in order to be effective against the types of explosives you are concerned about in the quantities you are concerned about, it generally imposes a fairly significant weight penalty on the cargo container. So up to now that has not been implemented. However——

Senator BOXER. What I would like to do, Dr. Albright, is get together with you, because I have other information with some folks who have come to me. So how about that. We will not go into it here.

Mr. ALBRIGHT. Sure, sounds good.

Senator BOXER. I think it is something we ought to look at.

These are a really good cargo security bill that, Mr. Chairman, was voted out of your Committee and it is just sitting there. And Senator Hutchison has really taken the lead on this cargo inspection. This whole notion of the Known Shipper deal I think was proven fairly faulty, if you do not mind my saying this, when we had a gentleman have his friend put him into a box and ship him from New York to Texas, Mr. McKinley. That kind of said a lot right there.

So I think we really have got to—hopefully, the House will take up this bill. We need to do a lot more about the cargo, because the Known Shipper thing is fine. You may have a company that becomes a known shipper after some period of time and then hires someone who puts something in. I think the trusted passenger idea, could work because as somebody who has flown for years and you know everything about them, which I hope you will be moving on that.

But this trusted shipper thing is not good, in my opinion. We need to have that bill come through because you are not in my view doing enough on this front.

I want to ask you about a couple of, if I might, California things, since I have you here and you cannot run away. San Francisco Airport has been trying to get a letter of intent. They want to install an in-line baggage screening system, and they are looking as to when that might happen. Do you have any information on that?

Mr. MCHALE. I believe, Senator, that we have already executed a letter of intent with San Francisco. I will just doublecheck that.

Senator BOXER. Oh, good.

Mr. MCHALE. I may have that here.

Senator BOXER. That is very good.

In San Jose we are having a problem. Senator McCain was talking about going to an airport thinking you are going to miss your plane because the lines are backed up. In San Jose they were supposed to have been staffed at a 423 level. They have never really had that. They are down about 100, and there is attrition, and I know several people myself who have actually gotten there an hour, hour and a half, and they missed planes.

Are you working with that airport to solve their problem? They are just—my God, it is named Mineta Airport.

Mr. MCHALE. I used to work directly for Senator Mineta, so yes, it has always been an airport of great——

Senator BOXER. Congressman Mineta.

Mr. MCHALE. Congressman Mineta, Secretary Mineta.

Senator BOXER. Secretary Mineta.

Mr. MCHALE. Actually, let me say I did misspeak. San Francisco, we do not yet have a letter of intent with them. That is something we have been working with them on.

Senator BOXER. Could you talk to me about that later in the week?

Mr. MCHALE. Yes, I will, absolutely.

Senator BOXER. And San Jose, you are working with them?

Mr. MCHALE. San Jose is one of the most challenging airports in the country because of its layout. It does not have really any room, particularly at one end of it, where there is a funnel that leads you

into both the airline ticket counters and immediately to the checkpoints. So the lines back up on each other.

Senator BOXER. Well, be that as it may. I agree, it is tough. But my question is, are you working with them actively, because things are not good there. Really, things are not good and people are missing planes.

Mr. MCHALE. We are working with them actively. We have worked with them on the design of their new terminal. We are trying to figure out ways, better layout ways of just handling those lines.

Senator BOXER. Good.

Mr. MCHALE. But there is just not enough room there, is really the problem.

Senator BOXER. Well, they are saying they do not have enough people working there, so look into that. They say they are 100 down, that has hurt. First you have a problem because your layout is not good, and then you do not have the people you are supposed to have.

Last question: Flight attendant training. We all know what happened that horrible day, September 11th, where the flight attendants were——

The CHAIRMAN. Murdered.

Senator BOXER. "Murdered" is the right word, yes. And flight attendants are really in the plane the first line of defense. Some of us have worked hard to have qualified pilots armed and I am glad that passed and hope you are moving along. But I am worried about the training. What is the timetable for getting the training completed? When is the rule on flight attendant security training going to be issued?

Mr. MCHALE. We have worked hard on a curriculum and the requirements of flight attendant training. One of the challenges we have got right now is actually the FAA authorization, reauthorization bill you mentioned, changes the rules quite considerably for that.

Senator BOXER. Right. They weaken them.

Mr. MCHALE. Changed it from compulsory to voluntary.

Senator BOXER. It weakened it.

Mr. MCHALE. It also causes us to do the training, pick up some of the cost of that. So part of what we are trying to deal with here is are we going to have a very different set of rules that we have to operate under in the next few weeks. So we are working——

Senator BOXER. So you are waiting to see the fate of that——

Mr. MCHALE. That is part of it, yes.

Senator BOXER.—aforementioned bill.

Mr. MCHALE. It would be a very different program.

Senator BOXER. Thank you.

The CHAIRMAN. Well, I want to thank you, Senator Boxer, for your obvious deep involvement in this issue and your expertise, and I thank you very much. I also share your concern about the San Diego Airport, given that so many of my constituents use that airport, particularly in this summer months, where I might say they are not well treated by the people of San Diego. But we have to work on that as a long-term issue.

But I do want to thank you, Senator Boxer, for your involvement. We would not have probably had this hearing if it had not been for you. We will be having hearings in the future on this issue.

Mr. McHale, the one thing I want to emphasize to you, we do not want to be surprised. If there are problems and there are issues, we want to be informed. We do not want to be surprised. We want to work with you. My view is that the work of TSA has been overall well, with the understandable problems that are associated with the formation of a huge Federal bureaucracy. But we also acknowledge we have a long way to go.

I hope you will work with Ms. Berrick in designing a way for us to gauge the progress or lack of progress as you move forward to a more efficient and professional organization.

Dr. Albright, if there is one thing I know about this issue, it is we need technology. We need technology. We predicted a long time ago that we would have some kind of system where people who are, quote, "trusted" could move right through, and we get hung up in racial profiling and all kinds of other issues, and they are understandable.

But I cannot see, frankly, from my eyesight any significant improvement in the process that passengers go through since the day that these procedures were installed. I will not say that. I have seen some improvement. Do not get me wrong. I do not see grandmothers and little teeny kids being frisked, as we did perhaps some time ago.

Senator BOXER. I am a grandmother and I get frisked.

The CHAIRMAN. But you do not look like one, Senator Boxer.

So we really need to focus on this technology, not only on the issue that was discussed in the closed hearing, but just to provide the American people who are using their primary mode of transportation outside of automobiles as a way of getting from one place to another with a certain confidence that they will be able to go in a safe and secure and yet expeditious fashion.

So I hope that you will be able to report back to us, Dr. Albright, some improvements that have been made.

Mr. McHale, again I would much rather hear about it than read about it.

Mr. MCHALE. Absolutely.

The CHAIRMAN. Because then obviously we have not done our respective jobs of oversighting and assisting and your job of keeping us informed and working with us.

It has been a very helpful hearing. I thank the witnesses and this hearing is adjourned.

[Whereupon, at 11:47 a.m., the Committee was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERNEST F. HOLLINGS TO CATHLEEN A. BERRICK

Budget Issues

Question 1. How much funding do you think they need to do the job right in Fiscal Year 2004?

Answer. We have not specifically evaluated the amount of funding TSA needs to adequately carry out its mission during Fiscal Year 2004. However, we identified that TSA faces the following three key funding and accountability challenges in securing commercial aviation: (1) focusing limited financial resources on the areas of highest priority; (2) ensuring that costs for aviation security enhancements are controlled; and (3) measuring the effectiveness of security initiatives already implemented to determine whether they are achieving intended results. The Department of Homeland Security received an appropriation of $3.7 billion for aviation security for Fiscal Year 2004. In addition, the Aviation and Transportation Security Act (ATSA) created a passenger security fee to pay for specified costs of providing civil aviation; however, the fee has not generated enough money to cover the costs. 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.

Due to 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. We have recommended that TSA apply a risk management approach to focus its limited resources to strengthen security in aviation as well as in other modes of transportation.[1] A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets. Implementing this approach would enable TSA to better support key decisions and link available funding with efforts that are of the highest priority. TSA has agreed with our recommendation and expects to complete the development and automation of its risk management tools by September 2004.

TSA has implemented numerous initiatives designed to enhance aviation security, but it has collected limited information on the effectiveness of these initiatives, particularly the passenger screening program. We have found that for its passenger screening program, TSA's performance data has been focused on progress in meeting deadlines mandated by ATSA, rather than on the effectiveness of the program. To measure the effectiveness of security initiatives already implemented, we have advocated that TSA develop outcome-oriented strategic goals and performance measures, and have recommended steps that TSA should take to strengthen its strategic planning efforts.[2] These steps include establishing security performance goals and measures for all modes of transportation, and applying practices that have been shown to provide useful information in agency performance plans.[3] Without information on the effectiveness of its programs and a process for prioritizing spending on security initiatives based on an assessment of threats and vulnerabilities, TSA and the public have little assurance regarding whether TSA is using its resources to maximize security benefits. TSA has agreed to our recommendations, and has reported that it is in the process of developing outcome-based performance measures for incorpora-

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

[2] 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).

[3] An annual performance plan is to provide the direct linkage between the strategic goals outlined in an agency's 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.

tion in its 5-year performance plan. TSA is also implementing several efforts to collect performance data on passenger screening.

Question 2. Does the reprogramming of more than $854 million in Fiscal Year 2003 funding by TSA have a negative effect on the mission of the agency as a whole?

Answer. As you are aware, TSA has a multi-faceted mission. It includes ensuring the security for all modes of transportation, including commercial aviation. Although we have not specifically examined the effects of TSA's reprogramming of $854 million on its mission, we believe that there are often consequences associated with reprogramming. The effect of reprogramming on an agency's mission depends on the amount of funds a program loses or gains and the criticality of the program or activity to the agency's mission. TSA's reprogramming was largely directed at paying for costs associated with hiring, training, and deploying screeners, and was done at the expense of transportation security research and development projects, primarily next-generation explosives detection systems. Consequently, although TSA was able to meet its mandate related to the deployment of screeners, other aspects of its mission, such as researching and developing new technologies, were delayed. In the past, we and the Department of Transportation's Inspector General identified that TSA needed to address some of the causes that may have contributed to its reprogramming of $854 million in Fiscal Year 2003 funding. For example, we and the Inspector General recommended that TSA put in place the necessary infrastructure, including a cost accounting system, contract oversight, and risk management principles, to help prioritize its resources.[4] In response to these recommendations, TSA has taken some actions, including performing criticality, threat, and vulnerability assessments. We believe these efforts are a step in the right direction and warrant close monitoring by the Congress to ensure funds are appropriately spent.

Question 3. Has GAO done any evaluation of TSA's current staffing, its staffing standards, and the funding needed to perform this task efficiently each year?

Answer. GAO has two reviews underway that address TSA's efforts to adequately staff commercial airports with screeners. At the request of the House Subcommittee on Aviation, Committee on Transportation and Infrastructure, GAO is currently reviewing, among other issues, TSA's efforts to address airport-specific staffing needs, while reducing the screener workforce. We also recently initiated a review for this committee examining TSA's efforts to deploy its screener workforce to ensure the efficient utilization of electronic baggage screening equipment.

In September 2003, we issued a report on our preliminary observations on our passenger screeners review that we are conducting for the House Subcommittee on Aviation.[5] We reported that initially, screener staffing levels for all airports were developed by TSA headquarters without active input from the agency's Federal security directors who are responsible for overseeing security at each of the Nation's commercial airports. This led to staffing imbalances and concern by Federal security directors that they had limited authority to respond to airport specific staffing needs, such as reacting to fluctuations in daily and seasonal passenger flow. TSA officials acknowledged that their initial staffing efforts created imbalances in the screener workforce, and reported that as they work to further reduce the screener workforce, they will solicit input from the Federal security directors as well as airport and air carrier officials.

TSA also recently hired a consultant—Regal Decision Systems, Inc.—to examine its screener staffing levels at commercial airports. Based on Regal's study, TSA anticipates having a model for screener staffing that incorporates proven features that Regal has developed in its work for the Immigration and Naturalization Service (now the Bureau of Immigration and Customs Enforcement) Workforce Analysis Model (WAM). According to a TSA official, this model has been used to support the Immigration and Naturalization Service budgetary staffing analysis and builds upon existing TSA staffing models. We plan to complete our review of screener staffing levels and issue a report on our results by June 30, 2004.

GAO has also reported that TSA faces the challenge of strategically sizing and managing its workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures.[6] For our recently initiated review of the checked

---

[4] U.S. General Accounting Office, *Aviation Security: Progress Since September 11, 2001, and the Challenges Ahead,* GAO–03–1150T, (Washington, D.C.: Sept. 9, 2003); and U.S. General Accounting Office, *Aviation Security: Transportation Security Administration Faces Immediate Long-Term Challenges,* GAO–02–971T, (Washington, D.C.: July 25, 2002).

[5] 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).

[6] U.S. General Accounting Office, *Aviation Security: Efforts to Measure Effectiveness and Address Challenges,* GAO–04–232T (Washington, D.C.: Nov. 5, 2003).

baggage screener workforce, we will determine the impact of screener staffing levels on the effectiveness of baggage screening operations. As part of this review, we will determine to what extent TSA has implemented alternative baggage screening methods as a result of imbalances in screener staffing levels. We will also examine the impact of recent TSA screener workforce initiatives, such as cross-training passenger and baggage screeners and hiring part-time screeners, on the effectiveness of checked baggage-screening operations (*e.g.,* utilization of explosive detection systems). Finally, in a separate review, we plan to identify the potential impacts of installation of airport in-line checked baggage screening systems, (*e.g.,* reduced checked baggage screener staffing levels). We expect to issue reports on the results of these reviews in the spring of 2004.

Cockpit Security

Question 4. Has GAO looked at security training for flight attendants, what are your feelings concerning the ability of a group of hijackers to overpower the flight crew to get to the cockpit, and what does GAO believe needs to be done to improve the current training and the flight deck and cabin security procedures?

Answer. GAO has not conducted a review of the security training for flight attendants, or current security procedures employed by the flight deck and cabin crew. However, due to the importance of the flight deck and cabin crew's role in providing a last line of defense for security, and limited information on TSA's progress in this area, we believe a review of these issues would be valuable. Security provided by flight and cabin crew members is one element of TSA's layered approach to security that has not been closely examined.

GAO is aware that ATSA and the Federal Aviation Administration's (FAA) reauthorization act—Vision 100: Century of Aviation Reauthorization Act (as passed by the House and Senate)—include requirements for establishing security training for flight and cabin crew members. Specifically, ATSA required that not later than 60 days after enactment of the act, FAA and TSA develop detailed guidance for a scheduled passenger air carrier flight and cabin crew training program to prepare crew members for potential threat conditions. The act required that the program address the:

- determination of the seriousness of an occurrence,
- crew communication and coordination,
- appropriate responses to defend oneself,
- use of protective devices assigned to crew members (if such devices are required by FAA or TSA),
- psychology of terrorists to cope with hijacker behavior and passenger responses,
- live situational training exercises regarding various threat conditions,
- flight deck procedures or aircraft maneuvers to defend the aircraft, and
- any other subject matter deemed appropriate by FAA.

ATSA also requires that (1) FAA review, approve, or suggest revisions to the air carrier's proposed training program within 30 days of receiving the proposal, and (2) the air carrier complete the training within 180 days after approval from TSA.

FAA's reauthorization act (as passed by the House and Senate) would require that air carriers providing scheduled passenger air transportation carry out a training program for flight and cabin crew members to prepare them for potential threats. The program would be required to address the same elements as required by ATSA in addition to instruction on the proper commands for passengers and attackers and procedures for conducting a cabin search, including explosive device recognition. The act also would provide TSA with the discretion to decide whether to set minimum guidelines for airlines to follow, and would require the Under Secretary for Border and Transportation Security to develop and provide a voluntary advanced self-defense training program not later than one year after enactment of the Act.

Surface-to-Air Missile Defense

Question 5. How much is being spent to research what procedures and devices work and what won't work?

Answer. The Department of Homeland Security plans to spend $120 million during Fiscal Years 2004 and 2005 to support the development and demonstration of an antimissile device for commercial aircraft. Congress earmarked $60 million in FY04 for this ongoing effort in the conference report (H.R. Conf. Rep. No. 108–280) accompanying DHS' FY '04 appropriations act (PL 108–90). Additionally, both the House and the Senate introduced legislation (H.R. 580 and S. 311) that would (1) direct the Secretary of Transportation to issue regulations requiring all air carriers' turbojets to be equipped with a missile defense system, (2) require the Secretary to

purchase missile defense systems and make them available to all air carriers, and (3) establish certain interim security measures to be taken before the deployment of missile defense systems.

According to some estimates, there are nearly half a million "man-portable air defense" systems (MANPADs) in the world today. A single person can use these shoulder launched missiles to destroy aircraft, raising terrorism and other security concerns for the U.S. and international commercial aviation. Consequently, there are significant questions about the nature and effectiveness of U.S. and international efforts to control the proliferation of these weapons. We have a review underway for the House Armed Services Committee and the House Aviation Subcommittee that addresses several of these questions, including the (1) nature and extent of the threat from MANPADs, (2) effectiveness of U.S. controls on the use of exported MANPADs, (3) the ways in which multilateral efforts attempt to stem MANPAD proliferation, and (4) types of countermeasures available to minimize the threat of MANPADs and the cost of implementing these countermeasures. We plan to issue a report on the results of our review in March 2004.

Passenger Screening & Checkpoint Issues

Question 6. Does the cap of 45,000 full-time-equivalent screeners included in the Homeland Security Appropriations bill provide TSA the flexibility it needs to devise appropriate staffing levels for individual facilities?

Answer. A cap on TSA's full-time equivalent screeners limits the flexibility that TSA has to devise appropriate staffing levels for individual airports. TSA's current staffing model was developed using 45,000 screeners as the required outcome, rather than building a staffing allocation model based on actual needs. In September 2003, we reported that initially, TSA headquarters determined screener-staffing levels for all airports without actively seeking input from Federal security directors.[7] As mentioned earlier, this led to staffing imbalances and concern by Federal security directors that they had limited authority to respond to airport-specific staffing needs, such as reacting to fluctuations in daily and seasonal passenger flow. TSA officials acknowledged that their initial staffing efforts created imbalances and reported that as they work to further reduce the screener workforce, they will solicit input from Federal security directors as well as airport and air carrier officials.

TSA reported that they determined the current screener staffing levels using a computer-based modeling process that took into account the number of screening checkpoints and lanes at an airport; originating passengers; the number of airport workers requiring screening; projected air carrier service increases and decreases during calendar year 2003; and hours needed to accommodate screener training, leave, and breaks. TSA also recently hired a consultant—Regal Decision Systems, Inc.—to examine its screener staffing levels at commercial airports. The study is expected to be completed by the second quarter of 2004.

As part of our ongoing work on passenger and baggage screening, we are conducting a survey of all Federal security directors to obtain their input on staffing levels at airports, including whether they have the authority to respond to airport specific staffing needs. Additionally, we will continue to examine TSA's efforts to address airport-specific staffing needs, while reducing the screener workforce, and plan to issue a report by June 30, 2004. For our recently initiated review of the checked baggage screener workforce, we will also determine the impact of screener staffing levels on the effectiveness of baggage screening operations. We plan to issue a report on this review in the spring of 2004.

Question 7. How will TSA deal with the cap as air traffic returns to more normal traffic growth levels, and do you believe that this is a situation where budgetary issues may end up driving operational issues rather than the actual threat levels?

Answer. We believe that it will be a challenge for TSA to respond to traffic growth while operating at capped screener levels. Operating under these levels inherently limits TSA's flexibilities in responding to airport specific staffing needs. In an effort to overcome these limitations, TSA recently began hiring part-time screeners to adequately staff airports based on daily and seasonal fluctuations in passenger flow. Additionally, TSA anticipates that it will gain staffing efficiencies through implementing new security-enhancing technologies, processes, and procedures. For example, as explosive 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, may be reduced. Other planned security enhancements, such as the Computer-Assisted Passenger Prescreening System and the registered traveler program, also have the potential to make screening more efficient.

[7] See footnote 5.

Additionally, if airports choose to apply to opt out of the Federal screener program beginning in November 2004 and use their own or contract employees to provide screening instead of TSA screeners, a significant impact on TSA staffing could occur.

As part of our passenger screeners review, we currently are examining TSA's efforts to adequately staff airports, while reducing the overall size of the screener workforce. We also recently initiated a review of TSA's efforts to deploy its screener workforce to ensure the efficient utilization of explosive detection systems and explosive trace detection equipment. We believe the results of these reviews will identify the extent to which TSA can support airport security needs through available staffing.

Question 8. How many people does TSA need to process security checks at airports in the U.S. expeditiously?

Answer. While GAO has not independently determined the appropriate number of screeners TSA needs to process security checks at commercial airports, we are currently examining TSA's efforts to (1) address airport-specific staffing needs, while reducing the screener workforce, and (2) deploy its screener workforce to ensure the efficient utilization of electronic baggage screening equipment. As mentioned earlier, we believe these reviews will identify the extent to which available staff can support airport security needs. Additionally, TSA recently hired an outside consultant (Regal Decision Systems, Inc.) to conduct a study of screener staffing levels at various airports and expects the study to be completed by the first quarter of 2004. TSA is also continuing to review the staffing allocation provided through its initial modeling efforts to assess air carrier and airport growth patterns and will make adjustments as appropriate. We plan to review the results of these initiatives during our ongoing review.

Cargo Screening

Question 9. Does GAO believe that TSA's reprogramming of $61.2 million of its $75 million research and development (R&D) budget in Fiscal Year 2003 limits TSA's ability to sustain and strengthen aviation by making greater investments in R&D for more effective equipment to screen passengers, baggage, and cargo?

Answer. TSA's reprogramming of over 80 percent of its Fiscal Year 2003 research and development budget to help pay for staff salaries and other programs personnel costs during Fiscal Year 2003 could limit TSA's ability to sustain and strengthen passenger, baggage, and air cargo security. The reprogramming was largely directed at paying for costs associated with hiring, training, and deploying screeners and was done at the expense of transportation security research and development projects, particularly related to next generation explosive detection systems. For Fiscal Year 2004, TSA has been appropriated $ 155 million for R&D, of which the Conference Report (H.R. Conf. Rep. No. 108–280) earmarked $45 million for R&D on next-generation explosive detection systems and $55 million for air cargo security.

As you know, vulnerabilities exist in ensuring the security of cargo carried aboard commercial passenger and all-cargo aircraft. To reduce these vulnerabilities, 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.[8] 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 onto aircraft.[9]

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. 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. [10] We also 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 our recommendation and developed an air cargo strategic plan, which it released in November 2003. According to the plan,

---

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

[9] 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).

[10] See footnote 9.

TSA evaluated the feasibility of physically screening 100 percent of all air cargo and determined that limitations of technology and infrastructure make such an undertaking impractical, from both a flow-of-commerce and resource point of view. Instead, TSA plans to focus its currently available tools, resources, and infrastructure in a targeted manner to secure air cargo and to accelerate research and development of more effective and comprehensive tools for the future. For example, TSA is developing a Cargo Prescreening System that will take shipment data as well as information from the Known Shipper and other indirect air carriers databases and develop a risk score for that specific shipment based on terrorist watch list information, other intelligence, and advanced targeting algorithms. Because it will take time to develop the system, TSA will require that aircraft operators begin to randomly inspect cargo to be transported on passenger aircraft. TSA also plans to initiate a number of pilot projects to study the applicability of current and emerging non-intrusive cargo inspection technologies.

In our ongoing work, we are continuing to collect and analyze information on how TSA (1) spent transportation security research and development funds during Fiscal Year 2003, and plans to spend funds during Fiscal Year 2004, (2) determines and prioritizes research and development needs, (3) coordinates with and reaches out to Federal and private sector research and development organizations to understand available and emerging transportation security technologies, and (4) plans to accelerate the development and deployment of transportation security technologies. The results of our review will be reported to our requesters in the spring of 2004.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO CATHLEEN A. BERRICK

Question 1. In your opinion, has TSA been requesting a sufficient level of funding to carry out its mission? If not, where are the most dramatic shortfalls and what impact are insufficient resources having on the agency's ability to carry out its mission?

Answer. We have not specifically evaluated the amount of funding TSA needs to adequately carry out its mission during Fiscal Year 2004. However, we identified that TSA faces the following three key funding and accountability challenges in securing commercial aviation: (1) focusing limited financial resources on the areas of highest priority; (2) ensuring that costs for aviation security enhancements are controlled; and (3) measuring the effectiveness of security initiatives already implemented to determine whether they are achieving intended results. The Department of Homeland Security received an appropriation of $3.7 billion for aviation security for Fiscal Year 2004. In addition, the Aviation and Transportation Security Act (ATSA) created a passenger security fee to pay for specified costs of providing civil aviation; however, the fee has not generated enough money to cover the costs. 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.

Due to 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. We have recommended that TSA apply a risk management approach to focus its limited resources to strengthen security in aviation as well as in other modes of transportation.[11] A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets. Implementing this approach would enable TSA to better support key decisions and link available funding with efforts that are of the highest priority. TSA has agreed with our recommendation and expects to complete the development and automation of its risk management tools by September 2004.

TSA has implemented numerous initiatives designed to enhance aviation security, but it has collected limited information on the effectiveness of these initiatives, particularly the passenger screening program. We have found that for its passenger screening program, TSA's performance data has been focused on progress in meeting deadlines mandated by ATSA, rather than on the effectiveness of the program. To measure the effectiveness of security initiatives already implemented, we have advocated that TSA develop outcome-oriented strategic goals and performance measures, and have recommended steps that TSA should take to strengthen its strategic plan-

---

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

ning efforts.[12] These steps include establishing security performance goals and measures for all modes of transportation, and applying practices that have been shown to provide useful information in agency performance plans.[13] Without information on the effectiveness of its programs and a process for prioritizing spending on security initiatives based on an assessment of threats and vulnerabilities, TSA and the public have little assurance regarding whether TSA is using its resources to maximize security benefits. TSA has agreed to our recommendations, and has reported that it is in the process of developing outcome-based performance measures for incorporation in its 5-year performance plan. TSA is also implementing several efforts to collect performance data on passenger screening.

Question 2. Has GAO looked at where TSA is spending its research dollars in Fiscal Year 2003, and its plans for Fiscal Year 2004? Do they have enough funds to carry out an aggressive research program for things like biometrics and next general explosive detection systems?

Answer. We are currently reviewing TSA expenditures related to its transportation security research and development (R&D) program. This work was requested by the House Subcommittee on Aviation, Committee on Transportation and Infrastructure; the House Subcommittee on Homeland Security, Committee on Appropriations; the House Committee on Technology; and the Senate Committee on Governmental Affairs. According to our preliminary analyses, during Fiscal Year 2003, TSA was appropriated about $109 million for R&D, of which $74 million was for next-generation explosive detection systems. However, TSA reprogrammed about $61 million in R&D funding on next-generation explosive detection systems to help pay for staff salaries and other programs. For Fiscal Year 2004, TSA has been appropriated $155 million for R&D, of which the Conference Report accompanying the Fiscal Year 2004 Department of Homeland Security Appropriation Act earmarked $45 million for R&D on next-generation explosive detection systems.

According to TSA, the reprogramming resulted in TSA spending significantly less than planned during Fiscal Year 2003 on R&D projects such as biometrics and next-generation EDS. However, the funds that have been appropriated during Fiscal Year 2004 should permit TSA to carry out its plans to pursue new technologies, including biometrics and next generation explosive detection systems to scan for explosives at security checkpoints and to inspect air cargo. Our preliminary analyses of ongoing and planned TSA R&D projects has shown that there are numerous projects related to biometrics and next-generation explosive detection systems. We plan to continue to collect and analyze information on TSA's R&D program. The results of our review will be reported to our requesters in the spring of 2004.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERNEST F. HOLLINGS TO STEPHEN MCHALE

Access to Secure Areas

Passengers and aircrew members are screened when they enter the boarding areas, but airport employees, vendors, and contractors are not. Yet they have access to secure areas as well. TSA contends that screening airport employees, vendors, and contractors is "just too difficult."

Question 1. Why are airport employees, vendors, and contractors (and their personal belongings) not screened when they enter the airport security identification areas (SIDAs)/airport operations areas (AOAs)?

Answer. TSA is actively strengthening safeguards regarding access to Security Identification Display Area (SIDA) and sterile areas of our Nation's airports. Approximately 1.2 million aviation personnel including airport, airline, and vendor employees work in U.S. airports. More than 90 percent of these employees work in the Security Identification Display Area (SIDA) because they require access to aircraft to load luggage and cargo, provide catering services, fuel airplanes, perform maintenance, or serve as flight crew. Approximately 10 percent of these workers require access only to the airport sterile area, which is located past the screening checkpoint. The quantity of airport workers with SIDA credentials and the fact that they

---

[12] 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).

[13] An annual performance plan is to provide the direct linkage between the strategic goals outlined in an agency's 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.

have access to a wide variety of tools and equipment within the SIDA area represent significant challenges.

TSA agrees that those vendor employees that work in the sterile area of the airport should be physically screened as they have access to screened passengers, and has had Security Directives and Emergency Amendments in place for quite some time requiring this practice to be instituted. TSA is currently taking steps to address vulnerabilities in this arena by enhancing enforcement of this requirement and introducing enhanced measures to increase security in the SIDA and secure areas of the airports. Those measures include reducing the number of access points to the SIDA, increasing the number of random patrols by Law Enforcement Officers (LEOs) and more random identification checks. This approach is consistent with TSA's overall security strategy of a "system of systems," whereby each security ring contributes to TSA's overall security system but the overall system does not rely exclusively on any one component. In other words, the different security components complement and reinforce each other.

In applying this "system of systems" strategy to securing SIDA and sterile area access, TSA is also in the process of strengthening background checks for these workers. TSA currently requires fingerprint-based criminal history record checks of all airline and airport workers who have access to SIDA and vendor employees who work in the sterile area of an airport. In June 2004, TSA will begin conducting enhanced background checks on all commercial aviation workers in the U.S. who have access to the secure and sterile areas of our Nation's airports. This initiative will also include vetting new employees as they join the workforce, and the integration of newly available threat information. These enhanced checks will include advanced analysis of the best available information to determine whether an individual poses a potential terrorist threat. This initiative will focus on preventing known terrorists from gaining credentials allowing access to SIDA and sterile areas, thereby diminishing threats to our aviation system.

Information Dissemination

Question 2. TSA forwards security directives (SD's) and Information Circulars (IC's) to the airline corporate security departments, but it is my understanding that only American Airlines and UPS forward them directly to their Captains. Most airline corporate security managers still limit who gets them even though they are marked as "distribute to those with an operational need to know." Should airline Captains get "Security Directives" and "Information Circulars," which provide updated threat information, directly?

Answer. Security Directives (SDs) and Information Circulars (ICs) do not contain specific threat information. ICs contain information of concern to transportation security personnel, while SDs contain changes in procedures to security programs and/or plans. SDs and ICs are provided to the regulated party (*i.e.,* air carriers). The carriers have a responsibility to safeguard sensitive security information, but also distribution authority to forward to those with an operational need to know. Title 49 Code of Federal Regulations (CFR) § 1544.215 states that each aircraft operator must designate and use the pilot in command as the In-flight Security Coordinator for each flight to perform duties specified in the aircraft operator's security program. Those duties include reviewing pertinent security information for each flight with the ground security coordinator. It is the responsibility of the aircraft operator to keep both ground security and in-flight security coordinators properly informed, particularly with regard to threats and threat response as noted in 49 CFR §§ 1544.301 and 303.

Question 3. Are there any steps that you intend to take to improve this process?

Answer. TSA is working to simplify the language and framework of SDs to reduce the opportunity for misinterpretation. TSA expects aircraft operator ground security and in-flight security coordinators to perform their duties as assigned in the TSA approved aircraft operator's security program.

Flight Attendants

Question 4. The need for flight attendant training, which includes the ability of flight attendants to communicate discreetly with the cockpit, dates back to a White House Commission in 1999 on flight attendant injuries caused by unruly passengers and turbulence. The new types of dangers flight attendants face has sharply focused the need for this type of training. Why has flight attendant crew defense training not been adopted and funded?

Answer. TSA continues to pursue a dual solution to meet the needs of crew member security training. First, with respect to basic training, TSA is in the process of establishing new training standards. These standards will address all crew security training requirements including those found in Visionl00—Century of Aviation Re-

authorization Act (P.L. 108–76). TSA intends to issue the new standards in the late summer, 2004 to coincide with the approval of the New Common Strategy. In finalizing these standards, we will continue to seek input from the stakeholder community.

Second, TSA is in the process of finalizing a voluntary Advanced Crew Member Self Defense Program. As currently envisioned, this program will be approximately 24–28 hours in length, 85 percent of which will be hands on learning and practicing of self defense techniques. We are in the process of meeting with various stakeholders, including representatives of flight attendants, to receive input so we can finalize this curriculum. We intend to conduct five (5) prototype training sessions beginning in August 2004 and look forward to stakeholders participating and providing their feedback.

TSA is on schedule to meet the deadlines set forth in Vision 100 to establish an Advanced Crew Member Self-Defense Program and minimum standards for basic security training.

Budget Issues

Question 5. Each year, the Bush Administration's budget requests for TSA do not meet the agency's needs, and Congress is forced to bail TSA out with emergency funding. In addition, TSA has reprogrammed hundreds of millions of dollars within its budget which has created confusion and led to concerns about accountability and spending priorities within the agency. With an appropriation of $5.2 billion, do you believe that TSA is funded at the proper level for FY 2004?

Answer. TSA's final enacted appropriation for FY 2004 is $4.6 billion, and the funding level is proper and sufficient.

Question 6. Is TSA taking steps to commit monies in the coming Fiscal Year to those programs that were left underfunded due to reprogramming or a budget shortfall?

Answer. Current FY 2004 spending plans should address funding needs adequately in FY 2004 and FY 2005.

Explosive Detection System (EDS) Issues

In an effort to aid the installation of EDS, the FY 2004 Homeland Security Appropriations Act included $250 million for Letters of Intent (LOI) to place EDS in-line, and $150 million to procure more EDS machines.

Question 7. How many LOI requests have you received to date?

Question 8. Is the $250 million allocated for FY 2004 going to meet your needs for EDS installations this year?

Answer 7–8. As of the date of this hearing, TSA had issued six LOIs covering seven airports.

Additional Information: Since the hearing, two more LOIs were signed, bringing the total of eight LOIs covering nine airports. The $250 million allocated in FY 2004 for explosives detection system (EDS) installations will cover installment payments on these eight LOIs based on a 75 percent Federal contribution.

The President's FY 2005 budget proposal to the Congress requests funding to support the eight currently signed LOIs. While LOI's are an important tool to assist airports in realizing efficiencies in handling checked baggage, TSA also pursues other mechanisms that provide EDS technology to the airports. An additional 26 airports have expressed an interest in entering into an LOI with TSA for an in-line baggage screening solution.

At the current funding level, and applying the 75/25 cost share formula, TSA's FY 04 and FY 05 budget allocations for EDS installation can financially support:

- Reimbursement payments for the 8 existing LOIs (covering 9 airports);
- Installation and multiplexing of EDS equipment at the 9 LOI airports;
- EDS installation work needed at 13 airports that are building in-line systems; and
- Using FY03 FAA AIP grant money and EDS and ETD non-LOI installation work needed at airports to provide equipment capacity. The airports selected have a need for increased equipment capacity because of increased passenger loads and airport terminal expansion projects to support increases to air carrier service.

Cargo Screening

Question 9. TSA is moving ahead on an initiative to establish an Air Cargo Program this year for which Congress provided $85 million in the FY 2004 Homeland Security Appropriations Act. Of these funds, $30 million has been directed towards strengthening the agency's oversight of air cargo security, and $55 million has been

provided for air cargo security research and development (R&D) activities. What steps has TSA taken on this initiative to date?

Answer. *Known Shipper Program Enhancements:* TSA is currently enhancing the Known Shipper database which will allow verification of information and the authenticity of the entity from which the information is received. Enhancements include developing an automated Indirect Air Carrier (IAC) validation system that will allow us to better manage the program by providing the means to collect the data required to conduct criminal history records checks. The electronic system will replace the current labor intensive paper-based system, and will allow for immediate disqualification of noncompliant IACs. Furthermore, we are working with U.S. Customs and Border Protection to develop a compliance measurement program that will enhance the level of security, scrutiny and vetting of Known Shippers. Additionally, TSA is exploring the development of a freight assessment system that proposes to evaluate the risk associated with each shipment. Shipments deemed "high risk" will be identified for additional inspection before being transported on a passenger aircraft. As TSA does not currently capture this information, TSA is collaborating with CBP on the development of this program. TSA is hiring 100 air cargo inspectors to strengthen the field inspection workforce, in order to enhance regulatory compliance and supply chain security. TSA issued an announcement for these positions in November 2003 and is currently accepting applications.

Additional Information: Since this hearing, the funding provided in the Department of Homeland Security Appropriations Act, 2004 (P.L. 108–90) enabled TSA to hire 100 new cargo inspectors. All 100 cargo inspector positions have been selected, and paperwork is being processed by TSA Human Resources. We anticipate extending job offers to these applicants and bringing them on board by mid-2004.

Question 10. Air Cargo Canine Screening Pilot Program: TSA-certified explosives detection canine teams have been screening priority mail at eleven different airports across the country. Thus far the effective program has screened over 8.5 million pieces of mail. TSA-certified explosives detection canine teams have increased their efforts to focus on cargo areas and cargo shipments within the airport environment. Recently, the TSA Office of Aviation Operations (AVOPS) Cargo Group and the National Explosives Detection Canine Team Program (NEDCTP), in cooperation with DHS Customs and Border Protection, initiated a combined operation at eight U.S. airports in which outbound international cargo and aircraft were screened by TSA-certified explosives detection canine teams. TSA has initiated plans to conduct an Operational Test and Evaluation (0, T and E) to determine the effectiveness of TSA-certified explosives detection canine teams in order to facilitate the most efficient means of screening cargo with canines, while at the same time maintaining an acceptable detection rate. Over the next few months, the TSA NEDCTP staff will continue to work with other existing DRS programs in order to facilitate an efficient use of canine resources. What are your plans for the $55 million for R&D activities?

Answer. We have divided the $55 million for cargo screening research and development into three areas. The breakout is as follows:

- $26 million directed to the explosives detection system (EDS) air cargo inspection pilot program, which will deploy commercially available or non-developmental explosives detection equipment to airports to inspect high-risk cargo;
- $21.5 million directed for research and development to determine what existing technology can be used to build air cargo inspection systems; and
- $7.5 million directed for research and development to determine what existing technology can be used to build automated inspection systems for U.S. mail to be carried on a passenger aircraft.

Question 11. Members of Congress agreed during the development of ATSA, and later in the Homeland Security Act (PL 107), that Aviation Security affected both passenger airlines and cargo carriers. Did the TSA Cargo working group focus only on cargo security for passenger aircraft, if so, why?

Answer. No. In March 2003, TSA established a chartered internal Air Cargo Working Group (ACWG) to coordinate and unify TSA air cargo security initiatives for passenger and all-cargo aircraft through the development and implementation of a comprehensive strategic plan as recommended by GAO. This plan was completed and an executive summary released on November 17, 2003, and included as one of its four strategic objectives measures for securing the all-cargo aircraft through appropriate facility security measures. TSA is currently developing a Notice of Proposed Rulemaking to implement this strategic objective.

In developing the details of this objective, TSA relied heavily on the recommendation of the Aviation Security Advisory Committee (ASAC). ASAC is a standing committee organized under the Federal Advisory Committee Act and composed of ap-

proximately 30 non governmental organizations and Federal agencies. It was created in 1989 in the wake of the destruction of Pan Am 103 over Lockerbie, Scotland, to provide the Federal Government with expert consultation and advice on aviation security issues.

Question 12. What additional restrictions being established on shippers and passenger carriers?

Answer. On November 17, 2003, TSA issued two executive summaries, detailing restrictions on shippers and passenger carriers: (1) The Air Cargo Strategic Plan; and, (2) Security Directives to require random inspections of air cargo, and other security enhancements.

The Air Cargo Strategic Plan details a multiphased, risk-based blueprint for implementing a comprehensive air cargo security approach by applying existing capabilities and pursuing emerging technologies. TSA has tailored the air cargo security program to manage various security risks in a cost effective manner. It is based on the Department's goal of securing the air cargo supply chain, including cargo, conveyances and aircraft, through the implementation of a layered solution that includes: screening all cargo shipments in order to determine their level of relative risk; working with our industry and Federal partners to ensure that 100 percent of items that are determined to be of elevated risk are inspected; developing and ensuring that new information and technology solutions are deployed; and, implementing operational and regulatory programs that support enhanced security measures.

TSA's agenda for achieving this goal can be divided into four strategic objectives: (1) Enhance Shipper and Supply Chain Security; (2) Identify Elevated Risk Cargo through Prescreening; (3) Identify Technology for Performing Targeted Air Cargo Inspections; and, (4) Secure All-Cargo Aircraft Through Appropriate Facility Security Measures. The Air Cargo Strategic Plan will be supported by a Notice of Proposed Rule Making, which TSA will publish in the coming months, and accompanying specific programs and initiatives.

Random Screening Security Directives. The security directives require random inspection of air cargo and also require foreign all-cargo air carriers to comply with the same cargo security procedures that domestic air carriers must follow. Passenger aircraft that carry cargo and all cargo planes, both foreign and domestic, will be subject to the random inspections on flights within, into, and out of the United States. The carriers will conduct the inspections. TSA will ensure that inspections are completed properly.

Foreign all-cargo air carriers operating into and out of the United States also will be required to follow security plans approved by TSA which detail procedures for screening. In addition, plans will verify the identities of persons with access to planes and ensure the security of parked aircraft. The directives also outline reporting requirements for foreign air carriers should potential threats arise.

Passenger Screening and Checkpoint Issues

Question 13. A provision in the FY 2004 Homeland Security Appropriations bill that was signed into law by President Bush on October 1, 2003, maintains a cap on TSA's full-time staffing at 45,000 positions. TSA has been trying to meet this employment cap since it was first imposed, and over the last six months has cut more than 6,000 screener positions from its workforce. How many screening employees do you currently have?

Answer. As of November 1, 2003, the TSA screening workforce headcount of paid employees was approximately 45,600 full-time and part-time employees. Because this headcount includes part-time screeners, the number of Full-Time Equivalent (FTE) remained under the 45,000 FTEs cap. The use of part-time screeners provides Federal Security Directors with additional flexibility in scheduling screeners, allowing them to achieve greater efficiencies in matching capacity to the high and low periods of demand for screener services.

Question 14. Do you plan to make additional cuts?

Answer. TSA seeks to maintain as many screeners as necessary within the current 45,000 FTE statutory cap to provide adequate security screening at U.S. airports as required by law while maintaining a satisfactory level of customer service. As part of the overall review of the funds available for FY 2004, TSA will make every attempt to maximize resources for the screening operations payroll to meet airport security requirements.

While the overall size of the workforce is declining, TSA is also creating additional capacity by achieving greater efficiencies in the scheduling of screeners. Federal Security Directors at each airport now have access to scheduling tools that provide real-time information enabling them to forecast periods of peak demand for screening. TSA uses mores split shifts and has restructured the workforce to reach a high-

er ratio of part-time screeners to maximize operational flexibility. As a result of this restructuring, TSA can more efficiently schedule screeners to match capacity with the level of demand.

Question 15. Does the cap provide TSA the flexibility it needs to devise appropriate staffing levels for individual facilities?

Answer. TSA reviews the workforce requirements for each airport on a periodic basis. TSA has contracted with Regal to develop a "bottom-up" model designed to use airport-specific data to derive highly accurate staffing and throughput projections. This tool, once operational, will be an important asset in TSA's efforts to ensure that our screeners are deployed effectively to maximize the safety and security of the traveling public.

Question 16. How will TSA deal with the cap as air traffic returns to more normal traffic growth levels?

Answer. TSA monitors the recovery and growth of aviation traffic levels and will adjust for changing security needs. TSA will continue to work hard to achieve efficiencies in the screener workforce and maximize the use of available resources. To the extent that resources restrict our ability to provide security while maintaining a satisfactory level of customer service, we will inform the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and Congress of the probable impact. TSA will also suggest approaches to mitigate any adverse impact on effective security operations and work with Congress to reach solutions.

Question 17. Do you believe that this is a situation where budgetary issues may end up driving operational issues rather than the actual threat levels?

Answer. Our goal remains effective security, efficiently applied. Identifying the most appropriate level of resources to eliminate a specific security threat or mitigate a known vulnerability is a significant challenge. TSA continues to pursue risk assessment and vulnerability analysis to determine the most effective method of using scarce resources to protect the transportation system worldwide. In this way, we can make sure that we use available funds to achieve the most effective protection for the traveling public.

Currently, TSA has certification standards for checked baggage devices, but it is our understanding that there are no similar standards for carry-on bags or passenger screening.

Question 18. When do you expect to establish a certification standard for carry-on bags and passenger screening?

Question 19. How can we expect companies to develop solutions without these standards?

Question 20. What guidance are you giving to companies?

Question 21. How much funding will be available from the TSA for checkpoints, and what will be the time frame/mechanism for distributing it during FY04?

Answer 18–21. TSA has certification standards for the screening equipment it uses for carry-on baggage, including trace explosives detection devices that it uses for carry-on bags at screening checkpoints. TSA is also exploring new technology, and will be communicating Qualification Criteria and Specification Requirements for explosives detection technology to be used for carry-on baggage and persons through a Request for Proposal (RFP) solicitation. TSA has programmed $10.2 million from its FY 2004 Applied R&D appropriation for advanced checkpoint technology development and improvement to existing technologies. Additionally, $11.5 million of the FY 2004 Next Generation EDS R&D appropriation will be used for investigations into automated inspection for explosives in carry-on items, explosives detection trace portals for screening individuals, document scanners for detecting the presence of explosives residue on travel documents such as boarding passes, and use of quadrupole resonance for inspecting shoes and other carry-on items.

Question 22. On October 20, 2003, Mr. Nat Heatwole was charged with placing weapons on an aircraft. He carried box cutters and other dangerous items through checkpoints, and hid them aboard two Southwest Airlines aircraft. According to reports, this college student notified the TSA and yet no action was taken. Can you explain how the breach in security on the two Southwest Airlines planes occurred and how TSA plans to rectify this situation?

Answer. It would be inappropriate to discuss the specific details about this incident in a manner that could provide information on how security at our Nation's airports could be breached in the future. Instead, we will focus on the steps that TSA has taken to prevent similar incidents from reoccurring.

First, the channel through which TSA received the e-mail has been revised. TSA has swiftly changed procedures at its Contact Center and throughout TSA. Contact Center electronic mail, telephone calls, and other communications are filtered for se-

curity content, reviewed by a security analyst, and when appropriate, transmitted to our Transportation Security Coordinating Center and other units for action. Contact Center personnel are trained each month on how to identify potential security violations, threat information, and criminal activity conveyed through telephone calls or other means. In addition, all TSA employees and contractors have been given specific protocols to follow in identifying, documenting, and reporting potential threat communications.

TSA continually assesses vulnerabilities and adjusts plans for screener improvement. In July 2003, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, we gathered data from multiple sources to determine the actual, current level of performance and the root causes for the gap between desired and actual performance.

Based upon the Screener Performance Improvement Study, TSA worked closely with the BTS Directorate to identify an array of specific follow-up actions. These enhancements are now being implemented under TSA's Short-Term Screening Improvement Plan, which includes the following elements:

- Increased Federal Security Director (FSD) support and accountability;
- Enhanced training for screeners and supervisors;
- Increased frequency of covert testing conducted by TSA's Office of Internal Affairs;
- Human performance improvements;
- Development and deployment of new screening technologies;
- Complete deployment of Threat Image Projection (TIP) systems;
- Expedited IT connectivity to checkpoints and training computers;
- Continuously updated Aviation Operations policies and procedures; and
- Improved workforce management, staffing, and scheduling.

Additional Information: On June 24, 2004, U.S. District Judge Paul Grimm sentenced Nathaniel Heatwole to two years supervised probation and a $500 fine. Nathaniel Heatwole must also serve 100 hours of community service and reimburse his parents for up to $500 in legal expenses.

Question 23. We have been informed that the TSA is meeting with industry groups to set regulatory policy regarding aircraft security? Who has been included in these meetings and why?

Answer. When TSA was being stood up, TSA held meetings with airline industry groups such as Air Line Pilots Association, Air Carrier Association, Air Transport Association, American Association of Airport Executives, Airports Council International-North America, and Regional Airline Association to better understand existing regulatory policy in the area of aviation security. These meetings were instrumental for TSA to understand better the potential impact of possible security policies and regulations on the aviation community.

As a course of business, TSA meets regularly with carrier, airport, and employee associations to discuss security policies. In 2002, TSA assumed FAA's responsibility to lead the Aviation Security Advisory Committee (ASAC). ASAC, a standing body under the Federal Advisory Committee Act (P.L. 92–463), was created in 1989 in the wake of the crash of Pan Am 103 to provide the Federal Government with expert consultation on aviation security issues. Through this forum, TSA receives input from a wide ranging group of aviation associations regarding aviation security issues.

Question 24. Lines at Myrtle Beach Airport on weekends are averaging 40 minute waits. We have new carriers and new flights. In Charleston, SC, we are anticipating service from a new carrier that will require more screeners. We have only 100 screeners now, although we are supposed to have 110, and TSA is currently counting supervisors as line screeners. Charleston cannot even hire new people without TSA opening up an assessment center-a process that can take months to carry out. On top of that, TSA has threatened to fire people unless they agree to become part-time screeners, and many have since quit. We need to get this process straight. How many people does TSA need to process security checks at airports in the U.S. expeditiously?

Answer. TSA has contracted with Regal to develop a "bottom-up" model designed to use airport-specific data to derive highly accurate staffing and throughput projections. This tool, once operational, will be an important asset in TSA's efforts to ensure that our screeners are deployed effectively to maximize the safety and security of the traveling public.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO STEPHEN MCHALE

Passenger Security Screeners

Question 1. Earlier this year, based on a TSA on-site assessment of passenger throughput at Honolulu International Airport, the Hawaii Department of Transportation, constructed additional passenger screening lanes in an effort to reduce the time passengers must wait for the screening process. Although six of these lanes were built at the direction of the TSA, no additional screeners were provided. As a result, passengers at Honolulu International Airport continue to suffer from long wait times. During the summer peak, wait times were as long as 90 minutes.

Even with this shortage of screeners, Hawaii was identified by TSA headquarters as an "overstaffed airport" and ordered to reduce its full time workforce.

How does TSA plan to resolve the staffing problems at Honolulu International Airport and ensure efficient and expeditious processing of passengers?

Answer. TSA continues to develop its expertise to make workforce decisions not only more attuned to the needs of different categories of airports, but also customized to individualized airport requirements. Factors considered in our staffing decisions include: lane counts at each airport to determine preliminary requirements for passenger screeners; baggage screening flow and configurations; the quantity and distribution of originating passengers; seasonal fluctuations in passenger flows; upcoming construction at airport facilities; changes in the quantity or frequency of air carrier service; and, variations in airline load factors. In order to adjust for mitigating factors at individual airports, TSA also gathers information on their needs from Federal Security Directors (FSDs), airport operators, and local community leaders.

TSA recognizes the need to create a more flexible workforce in order to match screener work schedules to meet fluctuations in originating passenger traffic. We are increasing the number of part-time screeners and using more split shifts to provide the necessary scheduling flexibility. TSA began FY 2004 with a screener workforce of approximately 47,500, which equates to approximately 45,000 FTE. As of mid-February, we have about 45,700 screeners, equating to 43,700 FTE, with 14 percent of the screener workforce as part-time.

A more flexible workforce allows TSA to better align throughput capacity with the needs of airports like Honolulu International Airport (HNL). TSA's staffing model was used to provide the HNL's FSD with that airport's FTE numbers and annual manpower hours. The FSD has researched the staffing at HNL to determine how many current full-time screeners at HNL must convert to part-time status, voluntarily where possible but involuntarily where necessary. Based on analyses of other airports and their staffing, it is estimated that between 20 to 40 percent of the total workforce at HNL will be converted to part-time work in order to maximize the effectiveness of the allotted FTEs in addressing peak periods of passenger screening. Like other airports where involuntary conversions must take place, employees who are affected will have priority consideration to convert back to full-time if and when such positions become available again.

TSA is continually monitoring screener workforce staffing at individual airports to determine where adjustments are needed. Regular communication with FSDs and stakeholders allow us to adjust the staffing levels to reflect changes in checkpoints and baggage screening processes, while remaining sensitive to screener workforce morale and performance issues.

Question 2. Funding for Explosive Detection Systems (Question requested by Hawaii Department of Transportation)

Honolulu International Airport, like other major airports, needs to move the TSA's Explosive Detection Systems (EDS) out of the lobby and into a permanent in-line installation in the baggage conveyor system. Fiscal Year 2004 funds were appropriated by the Congress for this purpose. Where on the priority list is Honolulu International Airport? Can you estimate when TSA will be in a position to offer Honolulu International Airport a Letter of Intent to address this problem?

Answer. TSA's top priority is security, and as such, TSA is focusing its available funding for EDS installation at those airports that have not yet fully achieved or cannot maintain compliance with the 100 percent electronic screening mandate for checked baggage. TSA continues to balance many competing priorities and continues to review its priorities to maximize the utilization of the funds available. Changes to passenger throughput demands, terminal modifications and airport expansions make fulfilling TSA's goal of 100 percent electronic baggage screening a constantly moving target TSA has set aside funding to support purchase and installation of EDS equipment into an in-line system currently funded through an FAA Airport Improvement Project (AIP) grant issued to HNL. TSA cannot currently support addi-

tional projects associated with in-line screening solutions at HNL through a Letter of Intent (LOI). TSA's EDS installation funding has been designated for the following projects:

- Reimbursement payments for the 8 existing LOIs;
- Installation and multiplexing of EDS technology at the 9 LOI airports;
- EDS installation work at 13 airports that are building in-line systems using FY 03 FAA AlP grant money (of which HNL is one of those airports); and
- EDS and ETD non-LOI installation work needed at airports to provide additional equipment capacity to ensure an airport can maintain 100 percent electronic screening capabilities. The airports selected in this category have a need for increased equipment support increases to air carrier service.

Question 3. Security Screening for Cruise Ship Passengers

Thousands of cruise ship passengers transfer to Honolulu International Airport, generally on Saturday mornings, for their flights back home. Over the next few years, three new cruise ships will call Hawaii home, and serve the Hawaii interisland trade.

In an effort to avoid further congestion and even longer passenger screening wait times at Honolulu International Airport, I understand the TSA has conducted preliminary discussions about the possibility of performing baggage screening for transferring airline passengers at the Port of Honolulu rather than at the airport. This screening service would require the positioning of TSA equipment and personnel at the pier, and would require airline staff coverage at that location as well. What are the TSA's recommendations on how to address this intermodal issue?

Answer. TSA is currently participating in two different prototype intermodal security initiatives that facilitate the transfer of baggage between cruise ship arrival ports and airports. These initiatives were proposed by the regions involved and developed cooperatively between local and Federal agencies.

In the first initiative, TSA screeners and equipment from the local airport are relocated to the port to screen checked baggage of returning cruise ship passengers. The receiving airline then transports the bags to the airport through a bonded security company. The goal is to alleviate the surge in the baggage screening process created by large numbers of cruise ship passengers arriving at the airport simultaneously.

In the second initiative, cruise ship staff collects checked baggage of returning passengers the evening before arrival, and attaches bar coded identification tags. The cruise ship then transfers the baggage to the airport through a bonded security company, where the baggage is entered into the existing airport TSA screening process for checked baggage. Again, as in the first initiative, the goal is to alleviate the surge in the baggage screening process created by a sudden influx of arriving cruise ship passengers.

Stakeholder outreach has been extensive and ongoing. TSA staff has weekly contact with cruise lines involved in the prototype program and the local airport Federal Security Directors to collect statistics on the number of passengers and the amount of baggage screened and to work out any issues or problems in the system. TSA also conducted an onsite survey of passengers disembarking from cruises who participated in the seamless baggage transfer prototype. Passenger feedback was overwhelmingly positive.

While preliminary results of both prototypes appear favorable, TSA is currently conducting a more extensive program analysis regarding the full impact of these initiatives on industry, TSA resources (both personnel and equipment), and the justification and capability to expand the prototype programs. These analyses will assist TSA to determine how best to address intermodal connection security issues of the type that you raised.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RON WYDEN TO STEPHEN MCHALE

On August 1, 2003, the Transportation Security Administration's (TSA) published a *Federal Register Notice* (68 Fed. Reg. 45265) concerning its plans to develop and implement a new version of the Computer Assisted Passenger Prescreening System, commonly known as "CAPPS II." I believe that this *Notice* was a positive first step in explaining to the public TSA's plans for CAPPS II, and in providing information needed to assess the program's potential impact on privacy. However, the *Notice* also left me with a number of questions as to how CAPPS II would operate. I believe

that the answers to these questions are crucial to understanding the nature and implications of the system TSA is proposing. My questions fall into six main areas.

Question 1. What Goes On in the "Risk Assessment" Portion of the Process

According to the explanation contained in the August 1 *Federal Register Notice,* CAPPS II will involve two main steps. The first step is authentication, in which the system will compare PNR data with data contained in commercial databases "for the sole purpose of authenticating passenger identity." The result will be a numeric score showing the confidence level that the identity the passenger provided is accurate.

The second step is the risk assessment. This is an area where I believe the explanations to date have been insufficient, making clarification essential.

Question 1a. The *Federal Register Notice* states that "[t]he risk assessment function is conducted internally within the U.S. Government." Does this mean that, for purposes of the risk assessment, CAPPS II will not in any way query or otherwise make use of commercial databases?

Question lb. If the risk assessment process does not involve making additional queries of commercial databases, then what information *does* it rely on? At a minimum, it appears that the risk assessment will involve checking to see if the passenger is on any Federal list of known or suspected terrorists, or persons with outstanding arrest warrants for violent crimes. But are there additional sources of information, inside or outside government, that the risk assessment will use? Or does the risk assessment simply produce a "yes or no" answer as to whether the passenger is already on a government list of persons considered dangerous?

Question 1c. Checking against existing government watch lists seems like a straightforward way of determining whether a passenger is already known as a terrorist or suspected terrorist. But according to the *Federal Register Notice,* the risk assessment process will do more than that-it will determine the likelihood that the passenger has "identifiable links" to known terrorists or terrorist organizations. How can the risk assessment process ferret out such links, if the information it relies on consists of existing government watch lists? Is it envisioned that the government will compile lists of all persons who have *any link* with a known terrorist or terrorist organization? Wouldn't this be an exceedingly broad list?

Question ld. For example, suppose that a passenger once shared an apartment or college dorm room with a person who is now on a U.S. list of known terrorists. Would the risk assessment capture this link? If so, how? Would the risk assessment process check commercial databases, which may contain records of the passenger's past addresses? Or is it envisioned that this passenger would already be on a government watch list, based on this solely on this possibly innocent link?

Question 1e. The *Federal Register Notice* says that CAPPS II will generate a "risk score" for each traveling passenger. Is this "risk score" the product solely of the risk assessment process, or does it does it take into account the results of the authentication step as well? If the latter, does it factor in any data or information from the authentication process other than the numeric authentication score?

Question lf. Suppose a passenger is *not* on a government watch list of known or suspected terrorists. Could the CAPPS II system nonetheless produce a high enough "risk score" to bar the passenger from flying?

Answer la–lf. Because of the sensitivity of the response, TSA would ask that it be permitted to respond in detail in a classified briefing to be provided at your convenience. However, as you know, the Department has been reviewing CAPPS II in light of the many constructive comments we have received on many issues related to your questions. At this point, the proposal for aviation passenger pre-screening is being reshaped to address those concerns. While it is still being developed, our fundamental goals remain unchanged in developing an effective security program for passenger pre-screening:

- Improve the security and safety of international and domestic travelers, as well as the public at large, by seeking to ensure in advance that airline passengers are not persons who are known to be involved in or associated with terrorism;
- Effectively allocate secondary screening resources;
- Move the majority of passengers more quickly through airport screening, in part by reducing the number of individuals selected for secondary screening; and
- Fully protect privacy and civil liberties.

This initiative is a priority for the Department and TSA, and we look forward to working with you to further the goals of the program.

Question 2. Process for Detecting and Correcting Mistakes

The *Federal Register Notice* states that a passenger will be able to request access to the PNR data CAPPS II contains on him/her, and to request the modification of that data if the passenger believes it is inaccurate. However, the *Notice* goes on to observe that because CAPPS II will not retain data on passengers for any significant time, in most cases there will be nothing for the passenger to obtain or correct.

Question 2a. This suggests that, while a procedure for accessing and requesting modifications to records may be important in other contexts, this approach really isn't very useful for addressing mistakes that may occur under CAPPS II. Does TSA agree that CAPPS II is going to require other types of redress procedures?

Answer. Yes. The specific design of a passenger redress process depends on the parameters of the passenger prescreening system which is employed. As noted in the above response, the Department is currently examining the CAPPS II program. However, the Department is committed to developing appropriate mechanisms for passenger redress and will not deploy a passenger pre-screening system without such mechanisms in place.

Question 2b. For example, if the system repeatedly flags a particular individual as suspicious, what options will that individual have to rectify the problem? Suppose the problem stems from inaccurate information in a commercial database, which results in a low authentication score for that individual. In such a case, accessing records held by the CAPPS II system would be useless. How will the system deal with mistakes of this kind?

Answer. An essential part of the redress process is the establishment of the Passenger Advocate. The Passenger Advocate is being designed to focus on assisting passengers who feel that they have been incorrectly or consistently prescreened. When a passenger submits a complaint, TSA will work to identify the root cause for the selection during prescreening. The Government, with the complainant's permission to observe and monitor the results of prescreening during the complainant's future flights, will work to analyze the results of prescreening. This analysis will determine if the complaint is related to prescreening or due to another part of the screening process (*e.g.,* random selection). If the complaint is related to prescreening, passengers will be afforded the opportunity to pursue redress through the Passenger Advocate, the TSA Privacy or Civil Rights Office and then, in turn, through the DHS Privacy Office or DHS Office for Civil Rights and Civil Liberties, as appropriate.

As with the No-Fly list redress procedures, TSA will work closely with other law enforcement and other government organizations to create procedures by which the government may identify and correct inconsistent data that derive from law enforcement or other government data systems in a timely manner.

Before the final redress process is completed, TSA will present its plans to the public in appropriate forums to receive advice and opinion and to help advertise the availability and purpose of the process.

Question 2c. What is the justification for exempting CAPPS II from the Privacy Act's data access and correction requirements?

Answer. To protect information in the CAPPS II system that is classified, SSI, or otherwise sensitive, TSA exempted the system from access and amendment as the Privacy Act permits. The passenger prescreening system is expected to contain not only airline-provided passenger data, but also information about how the system operates, which databases, intelligence sources and methods are being used, and information about persons on government watch lists whose identities cannot be revealed without compromising national and aviation security.

TSA does not consider the information in passenger name records (PNR) to be sensitive such that access to the individual must be denied. The August 1st notice does provide a procedure for individuals who wish to correct their own PNR data. With respect to correction of passenger information, PNR records in the passenger prescreening system likely would not be corrected with any meaningful results. Each time a passenger flies, a new "passenger name record" or PNR will be sent from the airline to the CAPPS II system and that PNR will be deleted shortly after the passenger completes his or her travel itinerary. Correction of longstanding errors in a particular airline's PNR for an individual (*e.g.,* one of that airline's frequent fliers) is best accomplished directly by the airline. As part of the development of the redress system, TSA will work with the airlines to develop the best procedure for correcting repeating errors in an individual's PNR data.

Question 3. Accuracy of the "Identity Authentication" Part of the Process

The *Federal Register Notice* states that "[o]ne of TSA's primary purposes in creating this new system is to avoid the kind of miscommunication and improper identification that has, on occasion, occurred under the systems currently in use. During

the test period, TSA hopes to confirm that the use of the CAPPS II program will significantly reduce improper identification."

However, a recent Associated Press article ("Feds Don't Track Airline Watchlist Mishaps," by David Kravets, July 23, 2003) reported that TSA does not keep information on the number of people who are misidentified and wrongly delayed or barred from flights under the current system.

Question 3a. Does TSA have any systematic way oftracking how often the current system makes mistakes?

Answer. TSA tracks possible inaccuracies in the current system that fall under our operational control, most notably complaints from passengers who suspect that they are improperly included on the "no fly list." However, other factors can cause a particular passenger to be inconvenienced but that the passenger will attribute to being a mistake, including random screening protocols, magnetometer alerts, or airline-generated concerns that are independent of TSA. TSA has established procedures within the Office of the Ombudsman to receive such complaints and to resolve them to the extent of their authority.

TSA does have a redress system for travelers who believe that they are improperly included on the No-Fly List. Currently, a traveler who contacts TSA regarding possible discrepancies within the current system are asked a series of questions to ascertain that the delay encountered in obtaining a boarding pass is No-Fly List related. The traveler is required to submit a written description of any problems encountered during the check-in process. Valid No-Fly List travelers are sent a traveler letter, along with a Passenger Identity Verification Form. The traveler must submit certified or notarized copies of three of the listed on the form that apply to the individual. Upon receipt of the Verification Form and certified or notarized documents, TSA will determine whether there is any threat to aviation or national security that would prohibit the individual from flying. TSA may conduct a background check in making this determination. If the traveler is cleared to fly, air carriers and other appropriate parties will be notified. The TSA Office of the Ombudsman will forward a letter to notify the individual of the results.

Question 3b. If not, how will TSA determine whether and to what extent CAPPS II will reduce the number of cases of mistaken identity?

Answer. As noted earlier, the Department is currently reshaping the CAPPS II program. The passenger prescreening system that is deployed will be designed to track the percentage of complaints about multiple occurrences of enhanced screening that are resolved because an individual has the same or a similar name as a person of interest but is not that person of interest. However, the details as to how this will work will depend on the parameters of the system which will be deployed.

Question 3c. To what extent will TSA make public the results of its testing on the accuracy of the identity authentication process? Will the public be permitted to see the numbers behind any claimed decrease in misidentification-and to evaluate the rate at which mistakes still occur under the new system?

Answer. As noted above, the Department is currently reshaping the CAPPS II program. To the extent that the passenger prescreening system utilizes an identity authentication process, TSA will communicate the results of the tests to the public, so long as the results do not contain classified or sensitive security information or may be disclosed only in an appropriate setting to protect the security of the system.

Question 4. Financial and Health Data

The *Federal Register Notice* states that the CAPPS II system "will not use measures of creditworthiness, such as FICO scores, and individual health records." However, this statement appears in the explanatory "Supplementary Information" section of the *Notice.* In what appears to be the official portion of the *Notice*—the part headed "DHS/TSA 010"—there is no reference to such a limitation.

Question 4a. What is the *legal effect* of the statement in the "Supplementary Information" section that CAPPS II will not use individual financial and health information?

Answer. This statement is a statement of policy; it is not intended to create enforceable rights on the part of passengers or legal restrictions on TSA. Nevertheless, it is a policy to which TSA would adhere in implementing the CAPPS II system, and this policy is reflected in the body of the Privacy Act notice, which excludes credit and health-related records from those TSA may collect under the *Notice* for purposes of CAPPS II. As the Department is currently reshaping the CAPPS II program, such a discussion may not be relevant to the passenger prescreening system that will be deployed.

Question 4b. Why is there no comparable statement in the body of the official Privacy Notice itself?

Answer. In fact, the Privacy Notice does contain a specific enumeration of the categories of records that maybe stored in the CAPPS II system of records. Credit records or health-related records are not on the list of specifically enumerated categories of records. Therefore, they are not included and, absent a change in the Privacy Notice (which would require re-publication in the *Federal Register*), will not be included in any revised passenger prescreening system.

Question 4c. The *Notice* makes the CAPPS II system "exempt from publishing the categories of sources of records." Why is TSA claiming this exemption? As a legal matter, wouldn't this permit TSA, a year or two down the road, to reverse its decision to refrain from using individual financial and medical data-and to start using such data without telling the public? How can the public rely on any current TSA description of what information the CAPPS II system will or will not use, if TSA is reserving the right to expand or modify the information it uses without any public notice or scrutiny?

Answer. This exemption was deemed necessary in light of the classified government records that were envisioned to structure the algorithms in the risk assessment engine. To the extent that the specific record sources became known, it would be that much easier to reverse engineer and thus defeat the system. Medical and financial records are not included in the enumeration of the categories of records to be used. As a matter of Privacy Act law, moreover, if TSA were to decide to change the categories of sources of records to include medical and financial records, it would be required to republish the system of records notice. Therefore, the scenario posed—using data without notifying the public-is not permissible under the law.

Question 5. Procedures for Future Changes to CAPPS II

As noted above, the *Notice* makes CAPPS II "exempt from publishing the categories of sources of records." It also gives the CAPPS II system a security classification of "classified, sensitive."

Given this classified status and the exemptions from the Privacy Act, could TSA modify significant aspects of the CAPPS II program without disclosing the changes to the public? To what extent would TSA have the ability, from a legal perspective, to depart from the CAPPS II system description set forth in the *Notice*? Could a future TSA elect to make changes regarding the scope or operational characteristics of the CAPPS II system—and do so secretly, without a formal and public regulatory process? How easily could the various representations and assurances made in the *Notice* be withdrawn?

Answer. No. The Privacy Act requires that agencies publish in the *Federal Register* a notice concerning the establishment of a system of records or a revision in a record system. See 5 U.S.C. § 552a(e)(4). Significant changes in the CAPPS II program would in all likelihood require a revision in the record system for the program. TSA is committed to fair information practices, which would include due notice to the public of any major changes in the passenger prescreening system. TSA has its own Privacy Officer to ensure adherence to these fair information principles. Furthermore, the Chief Privacy Office of the Department of Homeland Security must approve of any significant revisions in the CAPPS II Program that would affect privacy. Our agency is committed to devising an effective passenger screening program that protects personal privacy while ensuring the safety of air travel.

Question 6. Intended Future Link to Immigration Data

The *Federal Register Notice* states that "[i]t is . . . anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) program at such time as both programs become fully operational, in order that processes at both border and airport points of entry and exit are consistent."

Question 6a. If the sole mission of the CAPPS II system is to determine whether a passenger may pose a risk to aviation security, why does the system need to be linked with immigration data? Is it anticipated that CAPPS II may eventually be used not only for safeguarding aviation security, but also for enforcing immigration law—for example, for apprehending illegal aliens or visitors who have overstayed their visas?

Answer. Immigration databases may be vital in determining potential passenger risk, particularly as they provide details regarding individuals who are known and have already been rigorously processed for admission into the United States. Again, we would be pleased to address details in a classified briefing.

Question 6b. What are the specific "processes at both border and airport points of entry and exit" to which the *Notice* refers? What are the specific types of potential inconsistencies that TSA hopes to avoid by linking the CAPPS II and US–VISIT systems? Please provide some concrete examples of problems that could arise if the two systems were not linked.

Answer. TSA diligently prepared the *Notice,* as required, to highlight potential uses and linkages for the public. The processes in question are those related to granting admission and collecting arrival and departure information for certain non-immigrant visitors to the United States. In deploying a passenger prescreening system, DHS would want to use all available information to identify potential terrorists, as directed in Homeland Security Presidential Directive-6 and consistent with the Privacy Act and all relevant statutes. While no decision has been made to link these two systems, there is potential that an exchange of information between CAPPS II and US–VISIT will strengthen both systems and improve overall consistency of performance with regard to identification and assessment of alien visitors to the United States.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO STEPHEN MCHALE

Airport Screener Staffing Level

The Transportation Security Administration (TSA) continues to struggle with staffing. As you attempt to meet an artificial number of screeners, and have to cut an additional 4,000 to 5,000 employees this year, the lines continue to get longer. At Detroit, for example, waiting times no longer meet the 10 minute customer service plan that was originally touted by TSA, but instead are more than double that, and at times as long as almost 50 minutes.

Question 1. Have you developed staffing standards for airports, large and small and what is your expected wait time? (NOTE: Wait time assumptions greatly affect the number of screeners needed to process people. TSA is moving to hire more part-time people, but that is being done to meet the 45,000 screener cap, not to meet a staffing/processing standard time frame.)

Answer. The challenges in achieving the optimized quantities of screeners vary considerably airport by airport. TSA will continue to work with the Department of Homeland Security (DHS) and the Office of Management and Budget to maximize available resources against the many needs of transportation security.

While the overall size of the workforce is declining per Congressional direction [TS1], TSA is creating additional capacity through achieving greater efficiencies in the scheduling of screeners. Federal Security Directors (FSD) at each airport now have access to scheduling tools that provide real-time information enabling them to forecast periods of peak demand for screening. TSA uses more split shifts and part-time screeners to maximize the operational flexibility available to FSDs when scheduling screeners to satisfy varying levels of demand. As a result of reducing excess capacity at periods of lower demand, fewer Full Time Equivalents can be used to meet the workload.

Nevertheless, TSA continues to recruit and train screeners to fill vacancies at traditionally hard-to-fill and understaffed airports. We review on an ongoing basis the workforce requirements for each airport, considering the number, location, and mix of full-time and part-time screeners. We engage airport operators and air carriers to ensure that growth rates, changes in flight schedules, and other concerns are incorporated into our planning. TSA shares Congress' desire to ensure that our human capital is deployed effectively to maximize the safety and security of the traveling public.

General Aviation/Smaller Aircraft Access to Washington National Airport

Background

General aviation aircraft are currently prohibited from operating at Washington National Airport.

In addition, after September 11, air carriers were forced to terminate certain routes to Washington National due to security concerns as the Federal Government barred 19-seat aircraft from operating at DCA. This included Clarksburg-National and Lewisburg-National. The Aviation and Transportation Security Act mandates the Federal Aviation Administration develop procedures to secure the flight deck of commuter aircraft, which would make them eligible to operate at DCA in the future. It is not clear when FAA will act on this mandate.

Question 1. Assuming all security needs are met, when will TSA make a decision about allowing a limited amount of general aviation charter operations into National Airport?

Answer. *Section 823 of the Vision 100-Century of Aviation Reauthorization Act, P.L. 108–176; 117 Stat. 2490 (Dec. 12, 2003)* requires *the Secretary of DHS to develop a* security *plan to permit general aviation aircraft to operate into and out of*

Ronald Reagan Washington National Airport (DCA). Development of this plan is ongoing among the various Federal agencies engaged in securing the National Capitol Region, including TSA. DHS will be glad to provide the Committee with an update once the plan has reached an appropriate stage of maturity.

Question 2. Is the TSA working with the FAA on the developing security requirements for 19-seat commuter aircraft? Do you expect to eventually allow 19-seat commuter aircraft to resume operations into National Airport?

Answer. Because of the sensitivity of the response, TSA would ask that it be permitted to respond in detail in a classified briefing to be provided at your convenience.

○