United States General Accounting Office

GAO

Report to Congressional Committees

February 2004

AVIATION SECURITY

Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges

GAO-04-385

February 2004

AVIATION SECURITY

Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-385, a report to congressional committees

Why GAO Did This Study

The security of U.S. commercial aviation is a long-standing concern, and substantial efforts have been undertaken to strengthen it. One of these efforts is the development of a new Computer-Assisted Passenger Prescreening System (CAPPS II) to identify passengers requiring additional security attention. The development of CAPPS II has raised a number of issues, including whether individuals may be inappropriately targeted for additional screening, and whether data accessed by the system may compromise passengers' privacy. GAO was asked to determine (1) the development status and plans for CAPPS II; (2) the status of CAPPS II in addressing key developmental, operational, and public acceptance issues; and (3) other challenges that could impede the successful implementation of the system.

What GAO Recommends

GAO is making recommendations to the Secretary, Department of Homeland Security (DHS), to develop project plans, including schedules and estimated costs, to guide CAPPS II development; establish a plan for completing critical security activities; create a risk mitigation strategy for system testing; establish policies governing program oversight; and develop a process by which passengers can get erroneous information corrected. DHS generally concurred with the report and its recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-385. To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov or David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Key activities in the development of CAPPS II have been delayed, and the Transportation Security Administration (TSA) has not yet completed important system planning activities. TSA is currently behind schedule in testing and developing initial increments of CAPPS II, due in large part to delays in obtaining needed passenger data for testing from air carriers because of privacy concerns. TSA also has not established a complete plan identifying specific system functionality that will be delivered, the schedule for delivery, and estimated costs. The establishment of such plans is critical to maintaining project focus and achieving intended results within budget. Without such plans, TSA is at an increased risk of CAPPS II not providing the promised functionality, of its deployment being delayed, and of incurring increased costs throughout the system's development.

TSA also has not completely addressed seven of the eight issues identified by the Congress as key areas of interest related to the development, operation, and public acceptance of CAPPS II. Although TSA is in various stages of progress on addressing each of these eight issues, as of January 1, 2004, only one—the establishment of an internal oversight board to review the development of CAPPS II—has been fully addressed. However, concerns exist regarding the timeliness of the board's future reviews. Other issues, including ensuring the accuracy of data used by CAPPS II, stress testing, preventing unauthorized access to the system, and resolving privacy concerns have not been completely addressed, due in part to the early stage of the system's development. The following table is a summary of TSA's status in addressing the eight key issues.

Status of TSA in Addressing Key Issues as of January 1, 2004

Fully addressed	Yes	No	Fully addressed	Yes	No
Oversight board	✔		Unauthorized access prevention		✔
Accuracy of data		✔	Policies for operation and use		✔
Stress testing		✔	Privacy concerns		✔
Abuse prevention		✔	Redress process		✔

GAO identified three additional challenges TSA faces that may impede the success of CAPPS II. These challenges are developing the international cooperation needed to obtain passenger data, managing the possible expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system. GAO believes that these issues, if not resolved, pose major risks to the successful deployment and implementation of CAPPS II.

Contents

Tables

Figures

Abbreviations

CAPPS	Computer-Assisted Passenger Prescreening System
CAPPS II	Computer-Assisted Passenger Prescreening System II
DHS	Department of Homeland Security
TSA	Transportation Security Administration

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

February 12, 2004

The Honorable Ted Stevens
Chairman
The Honorable Robert C. Byrd
Ranking Minority Member
Committee on Appropriations
United States Senate

The Honorable John McCain
Chairman
The Honorable Ernest F. Hollings
Ranking Minority Member
Committee on Commerce, Science and Transportation
United States Senate

The Honorable C. W. Bill Young
Chairman
The Honorable David R. Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives

The Honorable Don Young
Chairman
The Honorable James L. Oberstar
Ranking Minority Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Adam H. Putnam
Chairman
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

The security of our nation's commercial aviation system has been a long-standing concern, and for over 30 years, substantial efforts have been undertaken to strengthen it. However, the tragic events of September 11, 2001—which began with the hijacking of four commercial aircraft—

showed that weaknesses in commercial aviation security continued to exist. Many changes have since been made to strengthen aviation security and reduce opportunities for terrorists to hijack or destroy commercial aircraft. However, as recent flight cancellations and other events from December 2003 through February 2004 have shown, the threat of terrorist attempts to use commercial aircraft to inflict casualties and damage remains. With thousands of daily flights carrying millions of passengers, ensuring that no passenger poses a threat to commercial aviation remains a daunting task.

One of the efforts underway to address this task and strengthen aviation security is the development of a new Computer-Assisted Passenger Prescreening System that is known as CAPPS II. The prescreening of passengers—that is, determining whether airline passengers pose a security risk before they reach the passenger screening checkpoint—is used to focus security efforts on those passengers representing the greatest potential threat. Since the late 1990s, prescreening has been conducted using a computer-assisted system that, based on certain criteria and behaviors, identifies passengers that may pose a higher risk to aviation security. These higher-risk passengers and their baggage are subject to additional and more thorough screening.

In response to the events of September 11, 2001, and the requirement set forth in the Aviation and Transportation Security Act[1] that a computer-assisted passenger prescreening system be used to evaluate all passengers, the Transportation Security Administration's (TSA) Office of National Risk Assessment is developing CAPPS II. Unlike the current Computer-Assisted Passenger Prescreening System (CAPPS)[2] that operates on airlines' reservation systems, CAPPS II will be operated by TSA. Further, it will perform different analyses and access more diverse data, including data from commercial and government databases, to classify passengers according to their level of risk. The development of CAPPS II raises a number of concerns, including whether individuals may be inappropriately targeted by the system for additional screening, and whether data accessed by the system may compromise the privacy of the traveling public.

[1]Pub. L. No. 107-71, § 136, 115 Stat. 597, 637 (2001).

[2]When initially developed under the Federal Aviation Administration, this system was known as the Computer-Assisted Passenger Screening system or CAPS.

We were requested by the Chairman, House Committee on Transportation and Infrastructure; the Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform; and mandated by Public Law 108-90[3] to assess aspects of the system's development, including safeguards put in place to protect the traveling public's privacy. (See appendix I for a listing of the specific aspects of the system and program challenges we were mandated to review.)[4] As agreed to with the House and Senate Committees on Appropriations; the Senate Committee on Commerce, Science and Transportation; the House Committee on Transportation and Infrastructure; and the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census we assessed the

- development status and plans for CAPPS II,
- status of CAPPS II in addressing the program challenges identified in Public Law 108-90, and
- additional challenges that pose major risks to the development and implementation of the system.

To address these objectives, we reviewed relevant CAPPS II program documentation on the status of the program's development as of January 1, 2004, and interviewed agency officials, air carrier personnel, commercial data providers, and privacy advocacy organizations to discuss the system's development, its anticipated operations, and challenges to its implementation. We also reviewed the system's planned use of data, and plans to protect the system and its data from misuse and unauthorized access. Our work was conducted in accordance with generally accepted government auditing standards. A detailed discussion of our scope and methodology is contained in appendix II.

[3]Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003).

[4]The Vision 100—Century of Aviation Reauthorization Act, Pub. L. No. 108-176, § 607, 117 Stat. 2490, 2568-69 (2003) contains a similar mandate to review CAPPS II after the Under Secretary for Border and Transportation Security, Department of Homeland Security (the parent agency of TSA), certifies the system. Because of similarities in the assessments we were asked to perform, we are addressing this report to the House Committee on Transportation and Infrastructure; Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census; House Committee on Government Reform; and all reporting committees identified by Public Laws 108-90 and 108-176. We will provide a second report on the CAPPS II program to these recipients within 90 days after the Under Secretary certifies the system.

Results in Brief

Key activities in the development of CAPPS II have been delayed, and TSA has not yet completed important system planning activities. Specifically, TSA is currently behind schedule in testing and developing initial increments of CAPPS II, due in large part to delays in obtaining passenger data needed for testing from air carriers because of privacy concerns. Initial operating capability—the point at which the system will be ready to operate with one airline—was originally scheduled to be completed in November 2003; however, TSA officials stated that initial operating capability has been delayed and its new completion date is unknown. TSA also has not yet established a complete plan identifying specific system functionality that will be delivered, the schedule for delivery, and the estimated costs throughout the system's development. Establishing such plans is critical to maintaining project focus and achieving intended system results. Project officials reported that they have developed cost and schedule plans for initial increments, but are unable to plan for future increments with any certainty due to testing delays.

As of January 1, 2004, TSA has not fully addressed seven of the eight CAPPS II issues identified by the Congress as key areas of interest, due in part to the early stage of the system's development. These issues relate to (1) the effective management and monitoring of the system's development and operation and (2) the public's acceptance of the system through the protection of passengers' privacy and enabling passengers to seek redress when errors occur. The Department of Homeland Security (DHS) has addressed one of the eight issues by establishing an internal oversight board to review the development of major DHS systems, including CAPPS II. DHS and TSA are taking steps to address the remaining seven issues, however, they have not yet

- determined and verified the accuracy of the databases to be used by CAPPS II,
- stress tested and demonstrated the accuracy and effectiveness of all search tools to be used by CAPPS II,
- completed a security plan to reduce opportunities for abuse and protect the system from unauthorized access,
- adopted policies to establish effective oversight of the use and operation of the system,
- identified and addressed all privacy concerns, and
- developed and documented a process under which passengers impacted by CAPPS II can appeal decisions and correct erroneous information.

In addition to facing developmental, operational, and public acceptance challenges related to the key areas of interest of the Congress, CAPPS II also faces a number of additional challenges that may impede its success. These challenges are developing the international cooperation needed to obtain passenger data, managing the expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system. We believe that these issues, if not resolved, pose major risks to the successful development, implementation, and operation of CAPPS II.

In order to address the shortcomings we have identified, we are making a number of recommendations to the Secretary of Homeland Security to strengthen CAPPS II project planning, develop plans to mitigate program risks, provide greater oversight of CAPPS II operations and use, and clarify passenger redress procedures.

We provided a draft of this report to DHS for its review and comment. In commenting on the draft report, the department generally concurred with the report and its recommendations, but expressed some concerns with the draft report's presentation of CAPPS II progress, international cooperation, and mission expansion. We considered the department's comments in finalizing the report, and made revisions where appropriate.

Background

During the past 30 years, the federal government has taken significant steps to strengthen the screening of passengers flying on U.S. commercial aircraft. With the increased number of aircraft hijackings that occurred during the late 1960s and early 1970s, the government directed that all passengers and their carry-on baggage be screened for dangerous items before boarding. During the 1990s, as the volume of passengers requiring screening and the awareness of the terrorist threat against the United States increased, a computerized system was proposed to help identify passengers posing the greatest risk to a flight so that they could receive additional security attention. In 1994, the Federal Aviation Administration provided funding to a major U.S. air carrier to develop such a computerized system for prescreening passengers.

This system, known as CAPPS, was implemented in 1998 and is in use today by most U.S. air carriers. CAPPS enables air carriers to separate passengers into two categories: those who require additional security scrutiny—termed "selectees"—and those who do not. When a passenger checks in at the airport, the air carrier's reservation system uses certain information from the passenger's itinerary for analysis in CAPPS. This

analysis checks the passenger's information against the CAPPS rules[5] and also against a government supplied watch list that contains the names of known or suspected terrorists. A passenger's selectee status is then transmitted to the check-in counter where a code is printed on the boarding pass of any passenger determined to require additional screening, and at the screening checkpoint, passengers who are selectees are subject to additional security measures. CAPPS currently prescreens an estimated 99 percent of passengers on domestic flights. Certain air carriers manually prescreen their passengers using CAPPS criteria.

The terrorist attacks of September 11, 2001, however, became the impetus for change in both the way in which passengers are screened and the entities responsible for conducting the screening. The Aviation and Transportation Security Act, passed in November 2001, directed that a computer-assisted passenger prescreening system be used to evaluate all passengers before they board an aircraft. The act also directed the creation of TSA within the Department of Transportation. TSA assumed responsibility for civil aviation security from the Federal Aviation Administration, and for passenger and baggage screening from the air carriers.[6]

Within TSA, the Office of National Risk Assessment was charged with developing CAPPS II in response to the act's requirement. TSA plans to begin operating CAPPS II with a single air carrier and then expand to other air carriers at dates to be determined. When fully developed, CAPPS II is envisioned to operate in the following manner.

1. During the reservation process, the passenger will be required to provide four pieces of information: full name, home address, home phone number, and date of birth.[7] This information will be entered into the Passenger Name Record[8] and sent electronically to CAPPS II.

[5]CAPPS rules are behavioral characteristics used to select passengers who require additional security scrutiny.

[6]The Homeland Security Act of 2002, Pub. L. No. 107-296, § 403, 116 Stat. 2135, 2178, transferred TSA from the Department of Transportation to the DHS.

[7]Some of this information may currently be collected during the reservation process.

[8]The Passenger Name Record contains data related to a traveler's reservations and travel itinerary, and is contained in an air carriers reservation system. Such data include the passenger's name, phone number, and form of payment.

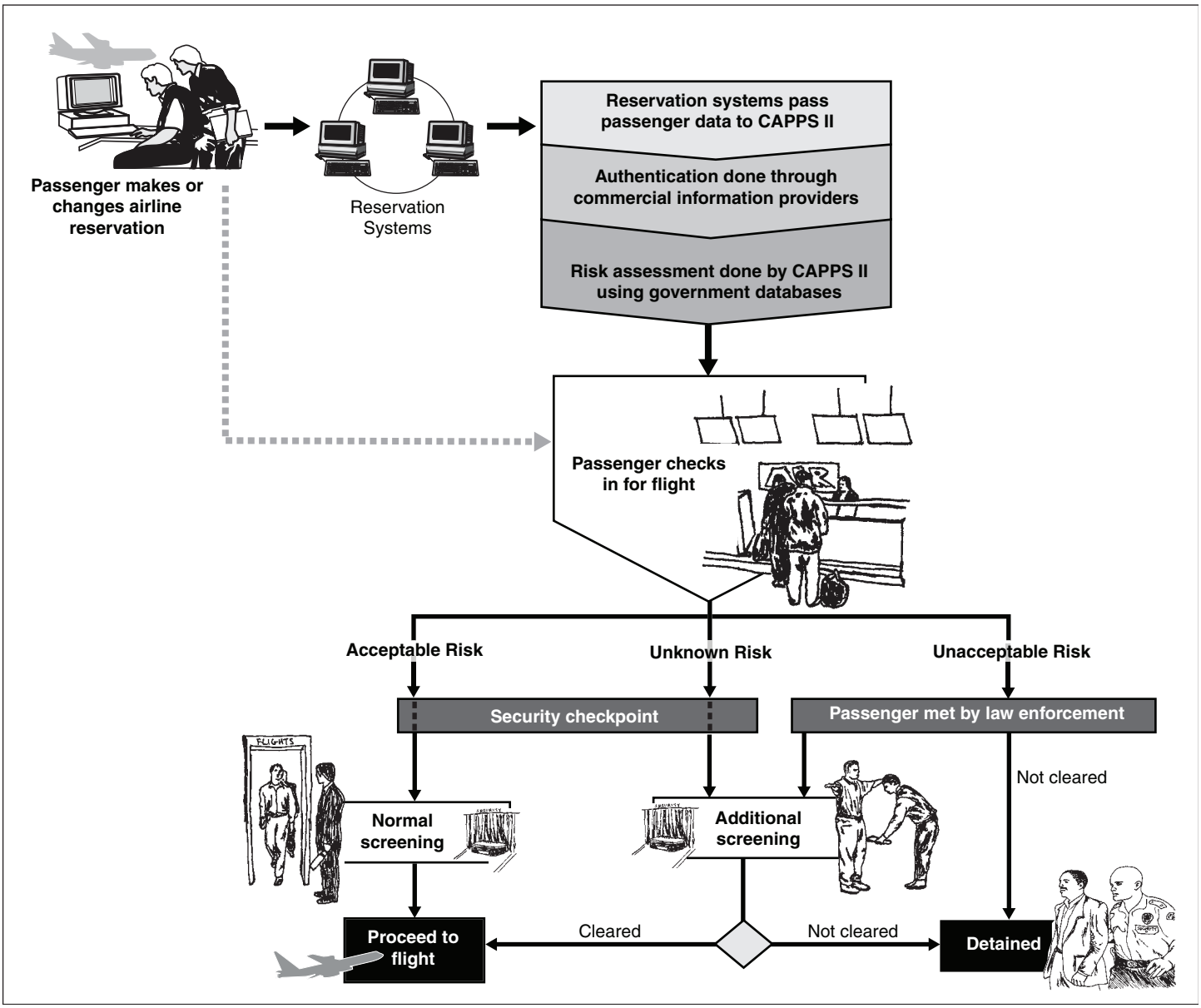
2. At a specified time prior to the flight, CAPPS II will request an identity authentication from commercial data provider(s), meaning that a passenger's personal information—full name, home address, home phone number, and date of birth—will be verified by information in the databases of one or more of the commercial data providers. Next, rather than the commercial data provider sending back any personal information, an identity authentication score will be returned to CAPPS II that identifies the level of confidence that the data provided by the passenger is authentic.

3. After obtaining passengers' authentication scores, CAPPS II will conduct risk assessments using government databases, including classified and intelligence data, to generate a risk score categorizing the passenger as an acceptable risk, unknown risk, or unacceptable risk.

4. When the passenger checks in for a flight at the airport, the passenger's risk category will be transmitted from CAPPS II to the check-in counter. Passengers who are an acceptable or unknown risk will receive a boarding pass encoded with their risk level so that checkpoint screeners will know the level of scrutiny required. If the passenger's risk is determined to be unknown, additional security checks will be required. Passengers whose risk assessment is determined to be unacceptable will not be issued boarding passes; instead, appropriate law enforcement agencies will be notified. Law enforcement officials will determine whether the individual will be allowed to proceed through the screening checkpoint or if other actions are warranted, such as additional questioning of the passenger or taking the passenger into custody.

Figure 1 displays the steps in the CAPPS II passenger prescreening process.

Figure 1: CAPPS II Passenger Prescreening Process



Source: GAO.

TSA program officials and TSA's draft Business Case for CAPPS II[9] state that the system will provide significant improvements over the existing CAPPS. For example, most air carriers currently use CAPPS within their reservation systems to assess passengers for possible risk, while CAPPS II will be owned and operated by the federal government. TSA believes that this consolidation will allow for more effective and efficient use of up-to-date intelligence information and make CAPPS II more capable of being modified in response to changing threats. In addition, TSA believes that CAPPS II has the potential to improve identity authentication. Another expected benefit of the system is the ability to aggregate risk scores to identify higher-risk flights, airports, or geographic regions.

Improved identity authentication could reduce the number of passengers who are falsely identified as needing additional security screening. Although exact numbers are not available, TSA officials estimate that currently 15 percent of passengers require additional checkpoint screening under CAPPS, compared to an expected 1 to 3 percent under CAPPS II.[10] CAPPS II is also ultimately expected to prescreen all passengers on flights either originating in or destined for the United States.

According to the draft Business Case for CAPPS II, the system has an estimated life cycle cost of over $380 million[11] through fiscal year 2008. Life cycle costs beyond fiscal year 2008 have not been estimated. According to program officials, approximately $41.5 million has been allocated for the system's acquisition to date.[12]

CAPPS II Development behind Schedule and Critical Plans Incomplete

Key activities in the development of CAPPS II have been delayed, and TSA has not yet completed key system planning activities. Specifically, TSA is behind schedule in testing and developing initial increments of CAPPS II, due in large part to delays in obtaining passenger data needed to test initial increments. Further, the agency has not yet established a complete plan identifying specific system functionality that will be delivered, the

[9]The draft Business Case outlines the system's proposed capabilities and system functions.

[10]Passengers can also be selected for additional security attention due to other reasons, such as setting off the alarm on the metal detector while being screened or being randomly selected.

[11]Life cycle costs do not include air carrier, reservation company, or passenger costs.

[12]These costs do not include $2.6 million the Department of Transportation spent on early system development or TSA's internal program management costs.

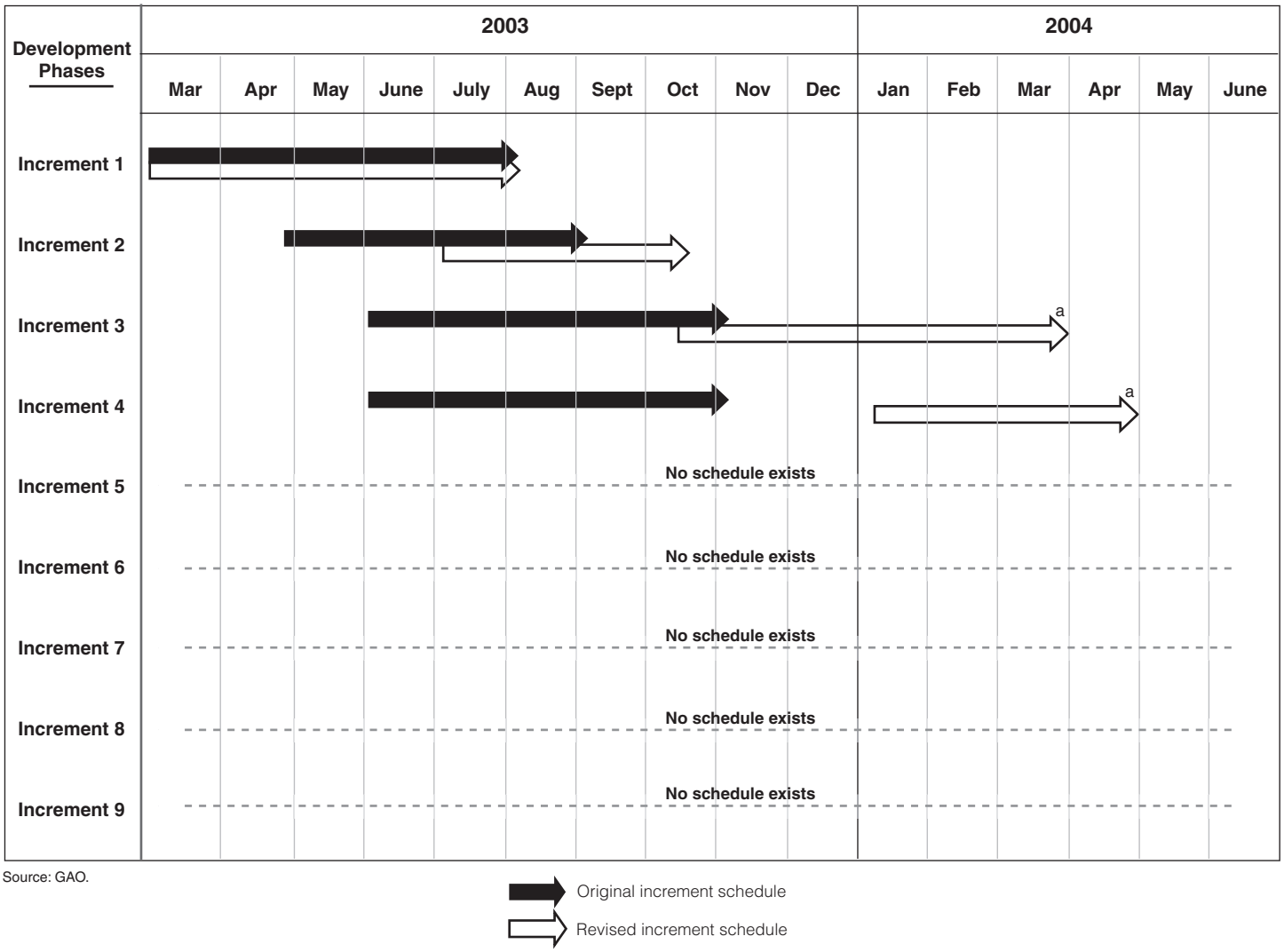
schedule for delivery, and the estimated costs throughout the system's development. Officials reported that due to testing delays, they were unable to plan for future increments with any certainty. The establishment of overall system requirements, a complete schedule of deliverables, and expected costs for each stage of development are critical to maintaining project focus and achieving intended system results and milestones within budget. Without such plans, TSA is at an increased risk of CAPPS II not providing expected functionality, of its deployment being delayed, and of incurring increased costs throughout the system's development

CAPPS II Is behind Schedule

TSA has encountered delays in the development of CAPPS II. TSA plans to develop CAPPS II in nine increments, with each increment providing increased functionality. (See appendix III for a description of these increments.) TSA planned to test each increment after it was developed to ensure the system met the objectives of that increment before proceeding to the next increment. TSA contracted to begin developing CAPPS II in March 2003 and completed increments 1 and 2 in August and October 2003, respectively. However, TSA has not fully completed testing these initial two increments because it was unable to obtain passenger data needed for testing from air carriers, which would not provide the passenger data because of privacy concerns. Instead, the agency deferred completing these tests until increment 3.

TSA is currently developing increment 3, and had originally planned to complete this increment by November 2003. However, due to the unavailability of passenger data needed for testing, TSA has delayed completion of this increment by five months and reduced the functionality that this increment is expected to achieve. Increment 3 was originally intended to provide a functioning system that could handle live passenger data from one air carrier in a test environment to demonstrate that the system can satisfy operational and functional requirements. However, TSA officials reported that they recently modified increment 3 to instead provide a functional application using a test simulator rather than an airline. Officials also stated that they were uncertain when the testing that was deferred from increments 1 and 2 to increment 3 will be completed. TSA recognizes that system testing is a high-risk area and plans to further delay the system's schedule to ensure that sufficient testing is completed. As a result, all succeeding increments of CAPPS II have been delayed, moving CAPPS II initial operating capability—the point at which the system will be ready to operate with one airline—from November 2003 to a date unknown. See figure 2 for a timeline showing the original and revised schedule for CAPPS II increments.

Figure 2: Timeline for Developing CAPPS II, by Original and Revised Increment Schedule



Source: GAO.

[a]System functionality to be achieved at revised schedule dates will be less than originally planned.

Critical CAPPS II Plans Are Not Complete

TSA has not yet developed critical elements associated with sound project planning, including a plan for what specific functionality will be delivered, by when, and at what cost throughout the development of the system. Our work on similar systems and other best practice research have shown that the application of rigorous practices to the acquisition and development of information systems improves the likelihood of the systems' success. In

other words, the quality of information technology systems and services is governed largely by the quality of the processes involved in developing and acquiring the system. We have reported that the lack of such practices has contributed to cost, schedule, and performance problems for major system acquisition efforts.[13] Sound project planning includes identifying specific functions to be delivered as well as the cost and schedule for delivering these functions.

TSA established plans for the initial increments of the system, including defined requirements for increments 1 and 2 and costs and schedules for increments 1 through 4. However, officials lack a complete plan identifying the specific functions that will be delivered during the remaining increments; for example, which government and commercial databases will be incorporated, the date when these functions will be delivered, and an estimated cost of the functions. In addition, TSA officials recently reported that the expected functionality to be achieved during early increments has been reduced, and officials are uncertain when CAPPS II will achieve initial operating capability—the point at which the system will be ready to operate with one airline. Project officials also stated that because of testing delays, they are unable to plan for future increments with any certainty.

By not completing these key system development planning activities, TSA runs the risk that CAPPS II will not provide the full functionality promised. Further, without a clear link between deliverables, cost, and schedule, it will be difficult to know what will be delivered and when in order to track development progress. Until project officials develop a plan that includes schedule milestones and cost estimates for key deliverables, CAPPS II is at increased risk of not providing the promised functionality, not being fielded when planned, and being fielded at an increased cost.

[13]U.S. General Accounting Office, *Major Management Challenges and Program Risks: A Government-wide Perspective*, GAO-03-95 (Washington, D.C.: January 2003) and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

Developmental, Operational, and Privacy Issues Identified by the Congress Remain Unresolved

TSA has not fully addressed seven of the eight issues identified by the Congress as key areas of interest related to the development and implementation of CAPPS II. Public Law 108-90 identified eight key issues[14] that TSA must fully address before the system is deployed or implemented. Taken together, addressing these issues will help ensure that (1) CAPPS II development and operation is effectively managed and monitored and that the system will function as intended and (2) the public has assurance that adequate measures exist to protect passenger privacy. Although TSA is in various stages of progress on addressing each of these eight issues, as of January 1, 2004, only one—the establishment of an internal oversight board to review the development of CAPPS II—has been fully addressed, as shown in table 1.

Table 1: Eight Key Issues Identified by Public Law 108-90 and the Status of Efforts to Address Them, as of January 1, 2004

Issues		
	Fully addressed	
Developmental and operational issues	**Yes**	**No**
1. Establish internal oversight board	✓	
2. Assess accuracy of databases		✓
3. Stress test system and demonstrate efficacy and accuracy		✓
4. Install operational safeguards to protect system from abuse		✓
5. Install security measures to protect system from unauthorized access		✓
6. Establish effective oversight of system use and operation		✓
Public acceptance issues		
7. Address all privacy concerns		✓
8. Create redress process for passengers to correct erroneous information		✓

Source: GAO analysis.

TSA program officials reported that they have not fully addressed these issues due to the early stage of CAPPS II development and not being able to obtain needed passenger data for testing, but reported that they are taking actions that they believe will ultimately address each issue. However, due to system development delays, uncertainties regarding when needed passenger data will be obtained, and the need to finalize key policy

[14]Pub. L. No. 108-90, § 519.

decisions, officials were unable to identify a time frame for when all remaining issues will be fully addressed. The following sections summarize the status of TSA's efforts to address each of the eight issues as of January 1, 2004.

Oversight Board to Monitor CAPPS II Development Has Been Established

Issue	Fully addressed	
	Yes	No
Establish internal oversight board	✓	

DHS created an oversight board—the Investment Review Board—to review the department's capital asset programs with contracts exceeding $50 million to ensure that projects meet mission needs at the expected levels of cost and risk. Comprised of senior DHS executives and chaired by the Deputy Secretary, the Investment Review Board is tasked with reviewing these programs—termed Level 1 investments—at key phases of program development, and reviewed the CAPPS II program in October 2003. As a result of the October review, the Board authorized TSA to proceed with the system's development. However, it noted some areas that the program needed to address. The Board identified concerns regarding privacy and policy issues, coordinating with other stakeholders, and identifying program staffing requirements and costs, among others, and directed that these issues be addressed before the system proceeds to the next phase.

Although DHS has the Investment Review Board in place to provide internal oversight and monitoring for CAPPS II and other Level 1 investments, concerns exist regarding the timeliness of future reviews by the Board. DHS officials acknowledged that the Investment Review Board is having difficulty reviewing all of the critical departmental programs in a timely manner. As of January 2004, DHS had identified about 50 Level 1 investments that would be subject to the Board's review. As the CAPPS II program proceeds, it will be important for the Investment Review Board to oversee the program on a regular and thorough basis to provide needed oversight.

Accuracy of CAPPS II Databases Not Yet Determined

Issue	Fully addressed	
	Yes	No
Assess accuracy of databases		✓

TSA has not yet determined the accuracy—or conversely, the error rate—of commercial and government databases that will be used by CAPPS II. According to commercial data providers and TSA officials, commercial data providers maintain certain information on the accuracy of their databases. However, since each commercial provider assesses accuracy with different measures and criteria, each company's accuracy information is not comparable across the industry or to any consistent standard. In addition, accuracy data for government databases is not systematically collected. As a result, TSA officials stated that they will develop and conduct their own tests to assess the overall accuracy of information contained in commercial and government databases. These tests are not intended to identify all errors existing within a database, but

rather assess the overall accuracy of a database before determining whether it is acceptable to be used by CAPPS II.

TSA is developing accuracy tests for commercial databases—which will compare a limited set of data known to be 100 percent accurate against the databases—and estimates that the tests will be ready for application before the system achieves initial operating capability. A senior program official said that because commercial data companies already perform their own data quality testing and evaluations, TSA expects that its testing, when conducted, will demonstrate that the accuracy of the databases are sufficient for CAPPS II purposes. However, if testing shows that commercial databases planned to be used are not of adequate accuracy, TSA will need to identify and work with other commercial data providers to test and use their data. TSA officials stated that they also plan to conduct other quality assessments of the database companies by assessing their practices for ensuring and improving data quality. Finally, since databases will be added throughout the system's development, accuracy testing will need to continue as additional government and commercial databases are used.

In addition to testing the accuracy of commercial databases, TSA plans to better ensure the accuracy of commercial databases by using multiple databases in a layered approach to authenticating a passenger's identity. If available information is insufficient to validate the passenger's identification in the first database accessed, then CAPPS II will access another commercial database to provide a second layer of data, and if necessary, still other commercial databases. This layered system, which relies on multiple databases, is expected by TSA to ultimately save resources because not all passengers would have to be checked against all data sources. TSA also plans to improve the overall accuracy of authentication scores through a process that targets errors such as misspellings and typographical errors. TSA officials stated that this process may help to differentiate passengers with similar names.

TSA program officials said that testing government databases for overall accuracy will be challenging. For example, TSA does not know exactly what type of information the government databases contain, such as whether a database will contain a person's name and full address, a partial address, or no address at all. Furthermore, a senior program official said that TSA has no indication of the accuracy of information contained in government databases. The official stated that using data without assessing accuracy and mitigating data errors could result in erroneous passenger assessments, and that government database accuracy and

mitigation measures will be completed before the system is placed in operation.

Although TSA plans to take measures to mitigate errors in commercial and government databases used by CAPPS II, TSA officials and commercial data providers stated that databases determined to have an acceptable level of accuracy will likely still contain errors. Consequently, in addition to using multiple databases and a process to identify misspellings to correct errors in commercial databases, TSA is also developing a redress process whereby passengers can attempt to get erroneous data corrected. However, it is unclear what access passengers will have to information found in either government or commercial databases, or who is ultimately responsible for making corrections. Additionally, if errors are identified during the redress process, TSA does not have the authority to correct erroneous data in commercial or government databases. TSA officials said they plan to address this issue by establishing protocols with commercial data providers and other federal agencies to assist in the process of getting erroneous data corrected. (TSA's planning for a CAPPS II redress process is discussed in further detail in a later section of this report.)

Stress Testing and Demonstration of System Efficacy and Accuracy Delayed Due to Lack of Data

Issue	Fully addressed	
	Yes	No
Stress test system and demonstrate efficacy and accuracy		✓

TSA has not yet stress tested CAPPS II increments developed to date or conducted other system-related testing to fully demonstrate the effectiveness and accuracy of the system's search capabilities, or search tools, to correctly assess passenger risk levels. Stress and system testing are critical mechanisms performed during each stage of a system's development to ensure that the system and its components meet requirements and user needs. TSA initially planned to conduct stress testing on an early increment of the system by August 2003. However, stress testing was delayed several times due to TSA's inability to obtain the 1.5 million Passenger Name Records it estimates are needed to test the system. TSA attempted to obtain the data needed for testing from three different sources—two U.S. air carriers and a global distribution service, also known as a reservation company—but encountered problems due to privacy concerns associated with its access to the data. For example, one air carrier initially agreed to provide passenger data for testing purposes, but adverse publicity resulted in its withdrawal from participation. Similar situations occurred for the other two potential data providers. TSA's attempts to obtain test data are still ongoing, and privacy issues remain a stumbling block.

Further, as TSA continues to develop the system, it will need to conduct additional stress testing. For example, there is a stringent performance requirement for the system to process 3.5 million risk assessment

transactions per day with a peak load of 300 transactions per second that cannot be fully tested until the system is further along in development. Program officials acknowledge that achieving this performance requirement is a high-risk area, and have initiated discussions to define how this requirement will be achieved. However, TSA has not yet developed a complete mitigation strategy to address this risk. Without a strategy for mitigating the risk of not meeting peak load requirements, the likelihood that the system may not be able to meet performance requirements increases.

Other system related testing to fully demonstrate the effectiveness and accuracy of the system's search tools in assessing passenger risk levels also have not been conducted. This testing was also planned for completion by August 2003, but similar to the delays in stress testing, TSA's lack of access to passenger data prevented the agency from conducting these tests. In fact, TSA has only used 32 simulated passenger records—created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data—to conduct this testing. TSA officials stated that the limited testing—conducted during increment 2—has demonstrated the effectiveness of the system's various search tools. However, tests using these limited records do not replicate the wide variety of situations they expect to encounter with actual passenger data when full-scale testing is actually undertaken. As a result, the full effectiveness and accuracy of the tools have not been demonstrated. Similarly, these 32 records are not a sufficient amount of data to conduct a valid stress test of the system.

TSA officials stated that they are continuing to seek needed passenger data for testing, but believe they will continue to have difficulty in obtaining data for both stress and other testing until TSA issues a Notice of Proposed Rulemaking to require airlines to provide passenger data to TSA. This action is currently under consideration within TSA and DHS. In addition, TSA officials stated that before the system is implemented, a final Privacy Act notice will be published. According to DHS's Chief Privacy Officer, this notice is expected to be finalized sometime after March 1, 2004, at the earliest. Due to the lack of test data, TSA delayed the stress and system testing planned for increments 1 and 2 to increment 3, scheduled to be completed by March 31, 2004. However, a TSA official recently stated that they no longer expect to conduct this testing during increment 3, and do not have an estimated date for when these tests will be conducted. Uncertainties surrounding when stress and system testing will be conducted could impact TSA's ability to allow sufficient time for

testing, resolving defects, and retesting before CAPPS II can achieve initial operating capability, and may further delay system deployment.

Security Plans That Include Operational and Security Safeguards Are Not Complete

Issue	Fully addressed	
	Yes	No
Install operational safeguards to protect system from abuse		✓
Install security measures to protect system from unauthorized access		✓

Ensuring that information systems contain safeguards to reduce opportunities for abuse, and have substantial security measures in place to protect against unauthorized access by hackers or other intruders, are two elements of an information system security program. Such a program typically involves policies, processes, and practices for protecting a system, its networks, and the facilities that house these systems, and for ensuring that personnel who work on these systems have undergone appropriate checks and have been provided appropriate access to the system's information. Because of schedule delays and the early stage of CAPPS II development, TSA has not implemented critical elements of an information system security program. Therefore, TSA does not yet have assurance that CAPPS II will be adequately protected from abuse, computer hackers, or other information security concerns.

The Federal Information Security Management Act,[15] Office of Management and Budget guidance,[16] and industry best practices describe critical elements of a comprehensive information system security management program. These elements include security policies, a system security plan, a security risk assessment, and certification and accreditation of the security of the system. Together, these elements help provide a strong security framework for protecting information technology data and assets. However, as of January 1, 2004, none of these four elements have been completed for CAPPS II. Each of these elements, and the status of TSA's efforts to complete them, is discussed below.

- Security policies are the primary mechanism by which management communicates its security views and requirements, and are a key element of a comprehensive information security management program. TSA security officials responsible for securing CAPPS II stated that they are developing a security policy specific to their office that is expected to incorporate system, personnel, and physical security controls. In the interim, officials reported that they are using relevant portions of TSA's information security policy, the Director of Central Intelligence Directives, the National Industrial Security

[15]Pub. L. No. 107-347, §§ 301-305, 116 Stat. 2946, 2946-61 (2002).

[16]*Management of Federal Information Resources*, OMB Circular A-130.

Program, and the Defense Information Technology Security Certification and Accreditation Process to guide CAPPS II security.

- System security plans provide an overview of the security requirements of the system, describe established controls for meeting those requirements, and delineate responsibilities and expected behaviors for all individuals who access the system. The CAPPS II security plan is currently in draft and is expected to be complete by the time initial operating capability is achieved. TSA officials stated that the security plan, when fully developed, will contain system security requirements, a security risk assessment, and plans for addressing security requirements. Although the draft CAPPS II system security plan contains sections on securing the system, personnel, and facility, the details of most sections are incomplete.

- Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls, and are required by the Federal Information Security Management Act. Moreover, by increasing awareness of risks, these assessments generate support for policies and controls, which helps ensure that policies and controls operate as intended. The CAPPS II security risk assessment was originally scheduled for completion in the January/February 2004 time frame. However, TSA officials stated that the assessment has been postponed due to CAPPS II development delays and has not been rescheduled.

- Certifying and accrediting a system as secure entails that the appropriate officials have the necessary information to make a credible risk-based decision regarding whether to place the system into operation. A TSA security official stated that TSA is planning a three-phased approach for certifying and accrediting CAPPS II: (1) the sensitive compartmental information facility containing CAPPS II is to be accredited by the Central Intelligence Agency in March 2004; (2) the two government networks CAPPS II is using to transfer secret and top secret data are to be accredited, again by the Central Intelligence Agency; and (3) the fully developed CAPPS II will be accredited by DHS at a date to be determined. The TSA security official stated that TSA is unable to schedule the final certification and accreditation of CAPPS II because of the uncertainty regarding the system's development schedule. The official also stated that CAPPS II must be fully developed so that TSA can perform the necessary tests for final accreditation.

While TSA has begun to implement critical elements of an information security management program, these elements have not been completed. The completion of the system security plan, security risk assessment, and certification and accreditation process are critical to ensuring the security of CAPPS II. Until these efforts are completed, there is decreased assurance that TSA will be able to adequately protect CAPPS II information and an increased risk of operational abuse and access by unauthorized users.

Policies for Effective Oversight of the Use and Operation of CAPPS II Are Not Developed

Issue	Fully addressed	
	Yes	No
Establish effective oversight of system use and operation		✓

TSA has not yet fully established controls to oversee the effective use and operation of CAPPS II. TSA plans to provide oversight of CAPPS II through two methods: (1) establishing goals and measures to assess the program's strengths, weaknesses, and performance; and (2) establishing mechanisms to monitor and evaluate the use and operation of the system. TSA has established preliminary performance goals and measures for CAPPS II; however, these measures may not provide all of the objective data needed to conduct appropriate oversight. In addition, TSA has not fully established or documented additional oversight controls to ensure that operations are effectively monitored and evaluated.

TSA has established preliminary goals and measures to assess the CAPPS II program's performance in meeting its objectives. The Government Performance and Results Act[17] requires that agencies establish goals and measures in order to appropriately oversee the performance of programs. As stated in TSA's draft Business Case for CAPPS II, the agency has established five strategic objectives with performance goals and measures, as shown in table 2.

[17]Pub. L. No. 103-62, 107 Stat. 285 (1993).

Table 2: CAPPS II Objectives, Performance Goals, and Measures

Fiscal year	Strategic objectives	Planned performance goal	Planned performance measure
2005	Establish automated system to prescreen all air travelers	77 Airlines (100%)	Percentage of 77 major commercial domestic airlines participating in CAPPS II
2005	Conduct automated prescreening of all passengers to determine potential risk of foreign terrorism	100% of daily passengers are prescreened	Percentage of daily passengers processed through CAPPS II
2005	Improve effectiveness of secondary screening by identifying those passengers representing a higher risk	CAPPS II efficiencies will result in approximately 60,000 passengers identified daily (3% of 2 million daily passengers) for increased screening	Number of passengers identified through CAPPS II
2005	Reduce passenger complaints about superfluous secondary screening	Percent of complaints about superfluous secondary screening resolved (to be determined after fiscal year 2004)	An increased level of passenger complaints about superfluous secondary screening is a direct indicator of adverse customer service; reducing the number of "false positives" will directly reduce the number of passenger complaints
2004 and 2005	Maximize accuracy of risk assessment	Fiscal year 2005 = 80% of referrals	Percent of referrals to law enforcement entities verified by law enforcement action to represent an increased risk

Source: TSA.

Goals and measures are intended to allow TSA and DHS management, other oversight bodies, and the Congress to systematically assess a program's strengths, weaknesses, and performance, and then identify appropriate remedies. In this regard, these preliminary goals and measures represent a good first step. They provide some useful intermediate performance information on key aspects of the program and, according to TSA, are tied to DHS and TSA strategic goals. We have previously reported that TSA had linked its aviation security goals to those of its then parent department, the Department of Transportation, and that linking goals of component organizations to goals of the parent organization are helpful in moving towards a results oriented culture and providing accountability for results.[18]

However, CAPPS II performance goals and measures could be strengthened. Two of the planned goals and measures are potentially

[18]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).

redundant, as the goal of prescreening 100 percent of passengers by 2005 will, by necessity, require meeting the goal of having all airlines participating in the system. Further, goals to improve the reliability and effectiveness of CAPPS II could be included. For example, although a performance measure is established for the percentage of referrals to law enforcement being verified as representing an increased risk, no goals or measures are established for assessing whether the system's performance is producing accurate scores and not producing errors, such as "false negatives"—when a passenger is not identified for increased screening when that passenger should have been. This is a key area for which TSA has acknowledged that data must be identified, quantified, and tracked for improvement. However, TSA has not developed a measure to assess its performance in this area. TSA officials stated that they are working with five universities to assess system effectiveness and management, and will develop metrics to be used to measure effectiveness of CAPPS II. With this information, officials expect to review and, as necessary, revise their goals and objectives to provide management and the Congress with objective information to provide system oversight.

In addition, TSA has not fully established policies and procedures to monitor and evaluate the use and operation of the system. TSA has built capabilities into CAPPS II to monitor and evaluate the system's operation and record actions taken by the program, and it plans to conduct audits of the system to determine whether it is functioning as intended. However, at this time, TSA has not written all of the rules that will govern how the system will operate. Consequently, officials do not yet know how these capabilities will function, how they will be applied to monitor the system to provide oversight, and what positions and offices will be responsible for maintaining the oversight. For example, TSA has not created all of the policies that will govern CAPPS II operations for compliance with privacy requirements. Until these policies and procedures for CAPPS II are developed, there is no assurance that proper controls are in place to monitor and oversee the system.

TSA Plans Address Privacy Protection, but Issues Remain Unresolved

Issue	Fully addressed	
	Yes	No
Address all privacy concerns		✓

TSA's plans for CAPPS II reflect an effort to protect individual privacy rights, but certain issues remain unresolved. Specifically, TSA plans appear to address many of the requirements of the Privacy Act, the primary legislation that regulates the government's use of personal information.[19] For example, in January 2003, TSA issued a notice in the *Federal Register* that generally describes the Privacy Act system of records[20] that will reside in CAPPS II and asked the public to comment. While TSA has taken these initial steps, it has not yet finalized its plans for complying with the act. For example, the act and related Office of Management and Budget guidance[21] state that an agency proposing to exempt a system of records from a Privacy Act provision must explain the reasons for the exemption in a published rule. In January 2003, TSA published a proposed rule to exempt the system from seven Privacy Act provisions but has not yet provided the reasons for these exemptions, stating that this information will be provided in a final rule to be published before the system becomes operational. As a result, TSA's justification for these exemptions remains unclear. Until TSA finalizes its privacy plans for CAPPS II and addresses such concerns, we lack assurance that the system will fully comply with the Privacy Act.

When viewed in the larger context of Fair Information Practices[22]—internationally recognized privacy principles that also underlie the Privacy Act—TSA plans reflect some actions to address each of these practices. For example, TSA's plan to not collect passengers' social security numbers from commercial data providers and to destroy most passenger information shortly after they have completed their travel itinerary appears consistent with the *collection limitation* practice, which states that collections of personal information should be limited. In addition, TSA's plan to prohibit commercial data providers from using information

[19]Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

[20]Under the act, a system of records is a collection of information about individuals under the control of an agency from which information is actually retrieved by an individual's name or by some identifying number, symbol, or other particular assigned to the individual.

[21]Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,972 (July 9, 1975).

[22]For purposes of this review, we used the eight Fair Information Practices proposed in 1980 by the Organization for Economic Cooperation and Development and that were endorsed by the U.S. Department of Commerce in 1981. These practices are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation, and accountability. See appendix IV for definitions of these practices.

they receive from TSA for commercial purposes appears consistent with the *use limitation* practice, which states that personal information should not be disclosed or used for other than the specified purpose except with consent of the individual or legal authority.

However, to meet its evolving mission goals, TSA plans also appear to limit the application of certain of these practices. For example, TSA plans to exempt CAPPS II from the Privacy Act's requirements to maintain only that information about an individual that is relevant and necessary to accomplish a proper agency purpose. These plans reflect the subordination of the *use limitation* practice and *data quality* practice (personal information should be relevant to the purpose for which it is collected) to other goals and raises concerns that TSA may collect and maintain more information than is needed for the purpose of CAPPS II, and perhaps use this information for new purposes in the future. Further, TSA plans to limit the application of the *individual participation* practice—which states that individuals should have the right to know about the collection of personal information, to access that information, and request correction—by prohibiting passenger access to all personal information about them accessed by CAPPS II. This raises concerns that inaccurate personal information will remain uncorrected in and continue to be accessed by CAPPS II.

Such actions to limit the application of the Fair Information Practices do not violate federal requirements. Rather, they reflect TSA's efforts to balance privacy with other public policy interests such as national security, law enforcement, and administrative efficiency. As the program evolves, it will ultimately be up to policymakers to determine if TSA has struck an appropriate balance among these competing interests.

See appendix IV for a more detailed analysis of TSA's plans to address privacy issues.

Redress Process under Development but Significant Challenges Remain

Issue	Fully addressed	
	Yes	No
Create redress process for passengers to correct erroneous information		✓

TSA has not yet finalized a redress process for passengers who are erroneously delayed or prohibited from boarding their scheduled flights, termed "false positives." According to TSA officials, a redress process for such passengers is a critical element of CAPPS II, and TSA intends to establish a process by which passengers who are subject to additional screening or denied boarding will be provided the opportunity to seek redress by filing a complaint. However, officials stated that such a program cannot be fully developed until key program policies are finalized, such as the length of time CAPPS II will retain passenger data and the conditions under which TSA will retain records longer than normal.

Although the redress process is not fully developed, TSA officials identified key elements they expect to include in the process. First, TSA will use its existing complaint procedures—currently used for complaints from passengers denied boarding passes—to document complaints and provide these to the TSA Ombudsman.[23] Complaints relating to CAPPS II will be routed to the Passenger Advocate, a position to be established within TSA for assisting individuals with CAPPS II-related concerns. The Passenger Advocate will represent the passenger and help identify errors in the system that may have caused a person to be identified as a false positive. Second, if the passengers are not satisfied with the response received from TSA with regard to the complaint, they will have the opportunity to appeal their case to the DHS Privacy Office. Third, TSA plans to conduct a public awareness campaign to inform travelers about what to expect from the new CAPPS II process and how to register complaints if they believe they are erroneously selected for additional security attention.

A number of key policy issues associated with the redress process, however, still need to be resolved. These include defining the role of the Passenger Advocate and the mechanisms that will be used to inform passengers of the outcomes of their complaints. More significantly, there are three concerns regarding data in CAPPS II that may complicate the redress process. These concerns involve data retention, access, and correction.

[23]The TSA Ombudsman is the designated point of contact for TSA-related inquiries from the public.

- Data retention: TSA has not yet determined how long CAPPS II will retain passenger data. Current plans indicate that data on U.S. travelers and lawful permanent residents will be deleted from the system at a specified time following the completion of the passengers' itinerary. Although TSA's decision to limit the retention of data was made for privacy considerations, the short retention period might make it impossible for passengers to seek redress if they do not register complaints quickly. TSA could rerun the passenger information through CAPPS II in an effort to recreate the deleted data, but TSA has no way of determining whether the results would be the same—the algorithms used to calculate risk scores change—or that risk scores were even the reason for the additional screening. Additional screening can be the result of factors such as setting off the alarm on screening checkpoint metal detectors or random selection, and not as a result of a risk score calculated by CAPPS II.

- Data access: TSA has not yet determined what information the Passenger Advocate will be able to share with passengers who file a complaint. Although TSA has stated that it is committed to providing access to information in CAPPS II to the greatest extent feasible, TSA officials stated that passengers will not have access to any government data used to generate a passenger risk score due to national security concerns. TSA officials have also not determined to what extent, if any, passengers will be allowed to view information used by commercial data providers.

- Data correction: TSA has not yet determined how the process of correcting erroneous information will work in practice. TSA documents and program officials stated that it may be difficult for the Passenger Advocate to identify errors. Further, it will be the responsibility of passengers to correct errors in commercial databases at their source, as TSA will refer the passengers to the original source of the data to seek correction. Correcting erroneous information is further complicated by the fact that commercial data providers may not be obligated to correct their databases, and that names of the data sources may not even be made available to the passengers due to licensing agreements.

To address these concerns, TSA is exploring ways to assist passengers who are consistently determined to be false positives. For example, TSA has discussed incorporating an "alert list" that would consist of passengers who coincidentally share a name with a person on a government watch list and are therefore continually flagged for additional screening. Although the process has not been finalized, current plans indicate that a passenger

would be required to submit to an extensive background check in order to be placed on the alert list. TSA stated that available remedies for all persons seeking redress will be more fully detailed in the CAPPS II privacy policy, which will be published before the system achieves initial operating capability.

Additional Challenges Could Affect the Successful Implementation of CAPPS II

In addition to facing developmental, operational, and public acceptance challenges related to key areas of interest to the Congress, CAPPS II also faces a number of additional challenges that may impede its success. We identified three issues that, if not adequately resolved, pose major risks to the successful development, implementation, and operation of CAPPS II. These issues include developing the international cooperation needed to obtain passenger data, managing the expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system.

International Cooperation

For CAPPS II to operate fully and effectively, it needs data not only on U.S. citizens who are passengers on flights of domestic origin, but also on foreign nationals on domestic flights and on flights to the United States originating in other countries. This information is critical to achieving the program's objective of reducing the risk of foreign terrorism and helping to avoid events like those of September 11, 2001. Moreover, as evidenced by the cancellation for security reasons of several flights to the United States from December 2003 through February 2004, the use of commercial aircraft originating in foreign countries may be the means terrorists choose to use to attempt future attacks.

To prescreen passengers on flights originating in foreign countries requires that CAPPS II obtain Passenger Name Record data on passengers from foreign countries, flying on foreign airlines, or purchasing tickets through foreign sources. However, obtaining international cooperation for access to this data remains a substantial challenge. The European Union, in particular, has objected to its citizens' data being used by CAPPS II, whether a citizen of a European Union country flies on a U.S. carrier or an air carrier under another country's flag. The European Union has asserted that using such data is not in compliance with its privacy directive and violates the civil liberties and privacy rights of its citizens. Its position extends not only to international flights to the United States, but also to U.S. domestic flights that carry citizens of European Union countries.

DHS and European Union officials are in the process of finalizing an understanding regarding the transfer of passenger data for use by the

Bureau of Customs and Border Protection for preventing and combating (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for these crimes. However, this understanding does not permit the passenger data to be used by TSA in the operation of CAPPS II but does allow for the data to be used for testing purposes. According to a December 16, 2003, report from the Commission of European Communities, the European Union will not be in a position to agree to the use of its citizens' passenger data for CAPPS II until internal U.S. processes have been completed and it is clear that the U.S. Congress's privacy concerns have been resolved. The Commission stated that it would discuss the use of European Union citizen passenger data in a second, later round of discussions.

TSA officials stated that in the short term, the lack of data on non-U.S. citizens could potentially affect the implementation of the system's initial operating capabilities. Moreover, officials stated that in the longer term, an inability to obtain data on non-U.S. citizens would hamper the effectiveness of the system. Without data on foreign nationals traveling to, from, and within the United States, CAPPS II would be unable to assess the threat posed by all individuals or by a group of passengers on a single flight, thus compromising the full capabilities and effectiveness of CAPPS II.

Expansion of Mission

Program officials and several privacy advocacy organizations have noted that the mission of CAPPS II may be expanded beyond its original purpose, and have expressed concern that this expansion may affect program objectives and public acceptance of the system. The primary objective of CAPPS II was to protect the commercial aviation system from the risk of foreign terrorism by screening for high-risk or potentially high-risk passengers, and to identify known foreign terrorists or their associates who are planning to board a flight. However, TSA has stated that it may expand the number of people targeted for additional security screening through CAPPS II. In the August 2003 interim final Privacy Act notice for CAPPS II, TSA stated that the system would seek to identify terrorists (both domestic and foreign) and not just foreign terrorists as previously proposed. The August notice also stated that the system could be expanded to identify persons who are subject to outstanding federal or state arrest warrants for violent crimes. Finally, in the notice, TSA also stated that CAPPS II could ultimately be expanded to include identifying individuals who are in the United States illegally or who have overstayed their visas.

DHS officials stated that they believe that such changes are not an expansion of the system's mission. Rather, they believe that the mission of CAPPS II is to strengthen aviation security, and as stated by the DHS Chief Privacy Officer, identifying wanted violent criminals and fugitives is consistent with that mission. DHS officials also stated that using CAPPS II to identify individuals not legally in this country is consistent with the broader DHS mission to protect the nation's borders from illegal immigration. However, focusing on persons with outstanding warrants, and possibly immigration violators, could put TSA at risk of diverting attention from the program's fundamental purpose, which is identifying persons who pose a threat to aviation security. Expanding the CAPPS II mission could also lead to an erosion of public confidence in the system, which program officials agreed is essential to the effective operation of CAPPS II. This expansion could also increase the number of passengers erroneously identified as needing additional security attention as well as the costs of passenger screening. Privacy advocacy organizations also expressed concern regarding the potential expansion of the CAPPS II mission to identify persons who are subject to outstanding warrants for violent crimes and illegal immigrants because they believe these individuals do not necessarily pose a threat to aviation security.

According to TSA program officials, the expansion of CAPPS II would also pose substantial operational challenges that they do not yet know how to effectively address. For example, implementing these possible changes could require integration with other data systems, such as the National Crime Information Center and immigration databases, as well as other databases that may contain data on persons with outstanding warrants. This would require involving additional agencies in the system, as well as additional equipment to effectively query these databases and integrate responses into CAPPS II. Further, TSA officials stated that some of these databases have reliability concerns, including the National Crime Information Center database. Recognizing these concerns, TSA officials reported that they are working to identify alternate sources of reliable data if CAPPS II were to be expanded as described.

Identity Theft

Another challenge facing the successful operation of CAPPS II is the system's ability to effectively identify passengers who assume the identity of another individual, known as identity theft. As our previous work has shown, identity theft appears to be growing in this country.[24] TSA officials

[24]U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

stated that while they believe CAPPS II will be able to detect some instances of identity theft, they recognized that the system will not detect all instances of identity theft without implementing some type of biometric indicator, such as fingerprinting or retinal scans. Successful identity theft would encompass two elements. First, an individual would have to obtain the personal identifiers (name, home address, date of birth, and home phone number) of an individual who would likely be classified by CAPPS II as an acceptable risk. Next, the person would have to obtain falsified documents associated with the stolen identity (such as a driver's license containing the stolen identifiers with the thief's picture) to present at the airport ticket counter and screening checkpoint.

TSA officials stated that while CAPPS II cannot address all cases of identity theft, CAPPS II should detect situations in which a passenger submits fictitious information such as a false address. These instances would likely be detected since the data being provided would either not be validated or would be inconsistent with information maintained by the commercial data provider. Additionally, officials said that identity theft and other fraud data may be available through credit bureaus, and that in the future they expect to work with the credit bureaus to obtain such data. However, they acknowledge that some identity theft is difficult to spot, particularly if the identity theft is unreported or if collusion, where someone permits his or her identity to be assumed by another person, is involved.

TSA officials stated that there should not be an expectation that CAPPS II will be 100 percent accurate in identifying all cases of identity theft. Further, they said that CAPPS II is just one layer in the system of systems that TSA has in place to improve aviation security, and that passengers who were able to thwart CAPPS II by committing identity theft would still need to go through normal checkpoint screening and other standard security procedures. TSA officials believe that, although not fool-proof, CAPPS II represents an improvement in identity authentication over the current system.

Conclusions

The events of September 11, 2001, and the ongoing threat of commercial aircraft hijackings as a means of terrorist attack against the United States, highlight the reasoning behind effectively prescreening airline passengers. An effective prescreening system would not only expedite the screening of passengers of acceptable risk, but would also accurately identify those passengers warranting additional security attention, including those passengers determined to have an unacceptable level of risk who would be immediately assessed by law enforcement personnel. CAPPS II, while

holding the promise of providing increased benefits over the current CAPPS system, faces significant challenges to its successful implementation. Uncertainties surrounding the system's future functionality and schedule alone result in the potential that the system may not meet expected requirements, may experience delayed deployment, and may incur increased costs throughout the system's development.

Of the eight issues identified by the Congress related to CAPPS II implementation, only one—establishing an internal oversight board—has been fully addressed. Of particular concern among the remaining seven issues is the security of both the system and passenger data contained in the system, as well as a means to provide adequate system oversight. Without proper oversight, there is limited assurance that the system and its data will be adequately protected against misuse, and that the system is operating as intended. Additionally, significant risks exist that adequate system testing, particularly to assure that CAPPS II can meet expected load demands, may be shortchanged. An effective risk mitigation strategy for system testing would help assure that system functionality and expected peak loads can be achieved. Lastly, given the concerns regarding the protection of passenger data, the system cannot be fully accepted if it lacks a comprehensive redress process for those who believe they are erroneously labeled as an unknown or unacceptable risk.

Recommendations

To address the challenges associated with the development, implementation, and operation of CAPPS II, we recommend that the Secretary of Homeland Security instruct the Administrator of the Transportation Security Administration to take the following seven actions:

- Develop plans identifying the specific functionality that will be delivered during each increment of CAPPS II, the specific milestones for delivering this functionality, and expected costs for each increment.

- Use established plans to track development progress to ensure that promised functionality is being delivered on time and within established cost estimates.

- Develop a schedule for critical security activities, including finalizing the security policy, the security risk assessment, and system certification and accreditation.

- Develop a strategy for mitigating the high risk associated with system and database testing that ensures (1) accuracy testing of commercial and government databases is conducted prior to the database being used and (2) appropriate stress testing is conducted to demonstrate the system can meet peak load requirements.

- Develop results-oriented performance goals and measures to evaluate the program's effectiveness, including measures to assess performance of the system in generating reliable risk scores.

- Develop policies and procedures detailing CAPPS II oversight mechanisms, including offices responsible for providing oversight, and reporting requirements for oversight information.

- Develop policies and procedures outlining the CAPPS II passenger redress process that include defining the appeal rights of passengers and their ability to access and correct personal data.

Agency Comments

We provided draft copies of this report to DHS for its review and comment. In a February 4, 2004, letter, the DHS Under Secretary for Management commented that the department generally concurred with the report and its recommendations. However, the Under Secretary provided the following comments related to CAPPS II development, international cooperation, and mission expansion.

First, the department does not believe that the report accurately describes its progress in developing CAPPS II. DHS acknowledged that the report discusses much of the system's progress in detail, but stated that the report's results in brief and summary charts do not characterize this progress accurately. Specifically, the Under Secretary stated that CAPPS II is not yet, nor could it be, at the point of having fully addressed many of the congressional areas of concern since it is still under development. Additionally, the Under Secretary stated that CAPPS II exists as a fully integrated, baseline functioning system that is not able to advance beyond its current state because the department is not authorized to receive passenger data.

We believe our description of the progress of CAPPS II is appropriate and balanced, and fairly describes the status of the system and its progress in achieving the requirements established by the Congress. Where appropriate, we provide DHS's perspective that the program is in an early stage of development. We also recognize throughout the report that delays in obtaining passenger data needed for testing has significantly impacted

CAPPS II development. However, we believe that the department's description of the system as being a fully integrated, baseline functioning system is misleading. The system has not yet been fully integrated with commercial and government databases. In addition, the system as it currently exists offers only limited functionality in a simulated environment, with additional functionality not to be added until later increments. DHS officials also recognized that they were uncertain when initial operating capability for CAPPS II would be achieved.

The department also expressed concern regarding the draft report's discussion of international issues as an impediment to CAPPS II deployment. Specifically, the Under Secretary stated that the draft report did not (1) clearly convey the complexity of the situation, (2) adequately convey the degree of international cooperation achieved, or (3) acknowledge that an agreement in principle with the European Commission permits the use of passenger data for testing CAPPS II.

We agree that international cooperation is a complex, multi-faceted issue. However, we believe that our report appropriately addresses this issue in sufficient detail as it relates to impediments to CAPPS II deployment and use. Further, presenting more information on this issue would require us to have discussed CAPPS II with other countries. However, as agreed to with DHS officials, we did not contact the European Union or other involved countries due to on-going negotiations with the United States regarding the use of foreign passenger data for CAPPS II. Thus, we included in the report information on international cooperation obtained from DHS and TSA officials as well as public documents from European Union organizations. However, based on our review of additional documentation provided by DHS, we revised our report to reflect that passenger data from European Union countries can be used for CAPPS II testing.

Finally, the department stated that the draft report was not accurate in asserting that the potential use of CAPPS II to detect individuals wanted for violent crimes or visa violations was an expansion of the program's mission. Moreover, the department states that differences between its January and August 2003 Privacy Act notices reflect limiting uses of personal information by CAPPS II.

We stand by the report's presentation on the potential expansion of the CAPPS II mission. Numerous TSA and DHS documents stated initially that the mission of CAPPS II was to protect the U.S. transportation systems and the public by conducting risk assessments to detect known and

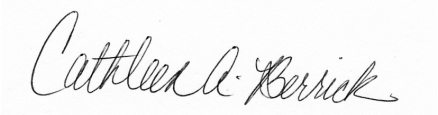
potential foreign terrorists. More recent documents added the potential purposes of CAPPS II to identify domestic terrorists, individuals with outstanding warrants for violent crimes, and individuals with potential visa violations. Further, the differences in the Privacy Act notices to which the department's comments refer focuses on routine uses—disclosures of personal information that the act permits "for a purpose which is compatible with the purpose for which it was collected." Contrary to the department's suggestion, the scope of a routine use does not, alone, describe the purpose of a system covered by the Privacy Act.

DHS also provided technical comments related to the program's development, status, and future plans. These comments were incorporated as appropriate.

The department's written comments are reprinted in appendix V.

We are also sending copies of this report to the Secretary of the Department of Homeland Security, the Administrator of the Transportation Security Administration, and the Director of the Office of National Risk Assessment. Copies of this report will be made available to others on request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions about this report, please contact Cathleen Berrick at (202) 512-3404 or Jack Schulze, Assistant Director, at (202) 512-4390. Questions concerning security and privacy issues should be directed to David Powner at (202) 512-9286, and Linda Koontz at (202) 512-6240, respectively. Major contributors to this report are listed in appendix VI.



Cathleen A. Berrick
Director, Homeland Security
and Justice Issues

David A. Powner
Director, Information
Technology Management Issues

Appendix I: Mandated Issues Contained in the Department of Homeland Security Appropriations Act, 2004

SEC. 519. a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Computer Assisted Passenger Prescreening System (CAPPS II) that the Transportation Security Administration (TSA) plans to utilize to screen aviation passengers, until the General Accounting Office has reported to the Committees on Appropriations of the Senate and the House of Representatives that—

1. a system of due process exists whereby aviation passengers determined to pose a threat and either delayed or prohibited from boarding their scheduled flights by the TSA may appeal such decision and correct erroneous information contained in CAPPS II;

2. the underlying error rate of the government and private data bases that will be used both to establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted;

3. the TSA has stress-tested and demonstrated the efficacy and accuracy of all search tools in CAPPS II and has demonstrated that CAPPS II can make an accurate predictive assessment of those passengers who may constitute a threat to aviation;

4. the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II is being developed and prepared;

5. the TSA has built in sufficient operational safeguards to reduce the opportunities for abuse;

6. substantial security measures are in place to protect CAPPS II from unauthorized access by hackers or other intruders;

7. the TSA has adopted policies establishing effective oversight of the use and operation of the system; and

8. there are no specific privacy concerns with the technological architecture of the system.

Appendix II: Scope and Methodology

To address our objectives, we reviewed documentation from the Transportation Security Administration's (TSA) Office of National Risk Assessment, and interviewed officials responsible for overseeing the development of the system, including associated contractors. We also interviewed officials at Department of Homeland Security (DHS) and TSA with oversight and implementation responsibilities for the Computer-Assisted Passenger Prescreening System II (CAPPS II), including the DHS Chief Privacy Officer, officials in the Office of Aviation Operations, and others responsible for CAPPS II oversight. In addition, we interviewed officials from privacy advocacy organizations, commercial database companies, air carriers, and other organizations that have knowledge of and/or concerns regarding CAPPS II.

To determine the status of CAPPS II's development and its related plans, we reviewed the CAPPS II draft Business Case, project schedules, planning documents, and associated system development documents. We also interviewed DHS and TSA program officials, as well as contractors associated with the development of CAPPS II.

To assess the status of CAPPS II in addressing the issues identified in Public Law 108-90, we did the following.

- To determine how the development and implementation of CAPPS II is overseen internally, we interviewed DHS and TSA officials with oversight responsibilities. We also reviewed available documentation of oversight mechanisms, such as the Investment Review Board.

- To determine whether TSA calculated database error rates and how the agency plans to mitigate those errors, we interviewed program officials and reviewed documentation on how TSA plans to assess data quality for CAPPS II. We also interviewed officials from several private database companies to discuss industry standards and practices for data quality and error mitigation.

- To determine whether TSA performed stress tests on the system and demonstrated the effectiveness and accuracy of CAPPS II search tools to make an accurate predictive assessment, we interviewed TSA officials to determine how the system is being designed and reviewed plans and procedures for stress and system testing. However, because the system is not yet operational, and TSA has not been able to obtain actual passenger data to conduct tests, no output results existed for us to review and analyze that would demonstrate whether CAPPS II would

be able to make an accurate predictive assessment of passengers who may pose a risk to aviation security.

- To determine what safeguards and security measures are in place to protect the system from abuse and misuse, we reviewed the system's draft security plans and TSA's security policies. We also interviewed TSA officials with system security responsibilities to determine what safeguards and security measures are planned and how they will function.

- To identify how TSA plans to oversee the use and operation of the system after implementation, we reviewed DHS and TSA policies and procedures governing oversight of the system. We also interviewed officials on how they plan to incorporate oversight mechanisms and performance measures into CAPPS II.

- To identify how agency officials are addressing Privacy Act requirements and other privacy-related issues, such as the Fair Information Practices, we analyzed agency documentation and interviewed agency officials with privacy-related responsibilities, including DHS and the Office of National Risk Assessment privacy officers. Based on our analysis of agency documentation and interviews, we assessed the extent to which CAPPS II is complying with the Privacy Act and following the Fair Information Practices. We also interviewed several privacy advocacy organizations, including the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, and the Electronic Frontier Foundation, to gain insight into domestic and international privacy concerns regarding CAPPS II.

- To determine whether a redress system for CAPPS II is planned and to describe it, we analyzed draft documents and working papers related to redress procedures for passengers identified for additional screening or denied boarding based on the CAPPS II risk assessment process. We also interviewed officials responsible for making policy decisions regarding redress procedures, including the DHS and TSA's Office of National Risk Assessment privacy officers, to obtain their input regarding planned redress processes.

To determine additional challenges TSA must address to successfully develop and implement CAPPS II, we interviewed and obtained relevant documentation from DHS and TSA regarding concerns and risks associated with the system's development. We used our prior reports and criteria we developed in reviewing similar systems. We also interviewed

privacy and public interest groups, as well as air carriers and airline associations, to obtain their perspectives on these challenges. The CAPPS II program also has international implications that may result in challenges to its implementation. However, due to ongoing discussions between the U.S. government and European Union regarding the use of data for CAPPS II, and the sensitive nature of these discussions, we did not discuss the system's development and implementation with representatives of foreign governments. We instead obtained information on international cooperation on CAPPS II from DHS and secured public documents from European Union organizations.

In reviewing CAPPS II and its development, we did not rely on computer-processed data and therefore did not conduct any data reliability assessments. We conducted our work from June 2003 through February 2004 in accordance with generally accepted government auditing standards.

Appendix III: CAPPS II Developmental Increments

The following describes general areas of functionality to be completed during each of the currently planned nine developmental increments of CAPPS II.

Increment 1. System functionality established at the central processing center. By completion of increment 1, the system will be functional at the central processing center and can process passenger data and support intelligence validation using in-house data (no use of airline data). Additionally, at this increment, validation will be completed for privacy and policy enforcement tools; the exchange of, and processing with, data from multiple commercial data sources; and processing of government databases to support multiple watch-lists.

Increment 2. System functionality established to support processing airline data. At the completion of increment 2, the system is functionally and operationally able to process airline data. Additionally, the system can perform functions such as prioritizing data requests, reacting to threat level changes, and manually triggering a "rescore" for individual passengers in response to reservation changes or adjustments to the threat level.

Increment 3. This increment will provide for a functional system that will use a test simulator that will not be connected to an airline's reservation system. System hardware that includes the establishment of test and production environments will be in place and a facility capable of performing risk assessment will be established. Design and development work for system failure with a back up system and help desk infrastructure will be put in place.

Increment 4. By this increment a back up location will be functionally and operationally able to support airlines processing application, similar to the main location. A help desk will be installed to provide assistance to airlines, authenticator, and other user personnel.

Increment 5. Enhanced intelligence interface. At the conclusion of this increment, the system will be able to receive from DHS the current threat level automatically and be able to adjust the system in response to changes in threat levels. The system will also be able to semi-automatically rescore and reclassify passengers that have already been authenticated.

Increment 6. Enhanced passenger authentication. This increment will allow the system to perform passenger authentication using multiple

commercial data sources in the instance that little information on a passenger is available from original commercial data source.

Increment 7. Integration of other system users. By the completion of this increment, TSA Aviation Operations and law enforcement organizations will be integrated into CAPPS II, allowing multiple agencies and organizations to do manpower planning and resource allocations based on the risk level of the nation, region, airport, or specific flight.

Increment 8. Enhanced risk assessments. This increment provides for the installation of capabilities and data sources to enhance risk assessments, which will lower the number of passengers falsely identified for additional screening. This increment also provides for a direct link to the checkpoint for passenger classification, rather than having the passenger's score encoded on their boarding pass.

Increment 9. Completion of system. Increment 9 marks the completion of the system as it moves into full operation and maintenance, which will include around-the-clock support, and administration of the system, database, and network, among other things.

Appendix IV: Detailed Information on TSA's Actions to Address CAPPS II Privacy Concerns

TSA's plans for CAPPS II appear to address many requirements of the Privacy Act, but certain issues remain unresolved. When viewed in the larger context of the Fair Information Practices that are internationally recognized and underlie the act, TSA's plans reflect actions to address each of these practices to at least some extent. However, in its efforts to balance privacy with national security and other public policy interests, TSA has proposed a number of actions which limit the application of certain of these practices and consequently, raise privacy concerns. Until TSA completes its privacy plans and the program is further developed, it cannot be determined whether the agency has identified all the CAPPS II privacy risks and taken actions to mitigate them.

TSA Plans Appear to Address Many Privacy Act Requirements, but Raise Concerns Pending Further Action

The Privacy Act of 1974 is the primary act that regulates the federal government's use of personal information. The act places limitations on agencies' collection, disclosure, and use of personal information.

At this early stage of program development, TSA has taken some initial actions to respond to the act's requirements for public notice. In January 2003, TSA issued (1) a notice in the *Federal Register* that generally describes the Privacy Act system of records[1] that will reside in CAPPS II and asked the public to comment, and (2) a proposed rule to exempt this system of records from seven Privacy Act provisions as permitted under the act. In August 2003, the agency issued an interim final notice in the *Federal Register* that describes planned changes to CAPPS II based on the public's comments on the January 2003 notice. The August notice also stated that TSA would issue a further Privacy Act notice before any implementation of CAPPS II.

Other initial TSA plans for CAPPS II are consistent with various Privacy Act requirements. For example, TSA plans to provide passengers with a Privacy Act notice that explains the authority for collecting their information, its principal purposes, and other information as the act requires. TSA also plans to perform real-time auditing and testing to identify data quality problems and improve accuracy. This appears consistent with the act's provision that agencies maintain only personal information that is accurate, complete, timely, and relevant. Our

[1]Under the act, a system of records is a collection of information about individuals under the control of an agency from which information is actually retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual.

assessment may change after TSA completes its privacy plans and the program is further developed.

While TSA has taken these initial steps, it has not yet finalized its plans for complying with the act. For example, the act and related Office of Management and Budget guidance[2] state that an agency proposing to exempt a system of records from a Privacy Act provision must explain the reasons for the exemption in a published rule. In January 2003, TSA published a proposed rule to exempt the system from seven Privacy Act provisions but has not yet provided the reasons for these exemptions, stating that this information will be provided in a final rule to be published before the system becomes operational. As a result, TSA's justification for these exemptions remains unclear at the present time. Until TSA finalizes its privacy plans for CAPPS II and addresses such concerns, we lack assurance that the system will fully comply with the Privacy Act.

TSA Application of the Fair Information Practices Reflect Efforts to Balance Privacy and National Security Goals

Fair Information Practices are a set of internationally recognized privacy protection principles. First proposed in 1973 by a U.S. government advisory committee, the Fair Information Practices are, with some variation, the basis of the privacy laws and related policies of almost every country that has addressed privacy protection, including the Privacy Act in the United States and similar laws in the European Union. For purposes of this review, we used the eight Fair Information Practices proposed in 1980 by the Organization for Economic Cooperation and Development that were endorsed by the U.S. Department of Commerce in 1981 as shown below:

1. *Collection limitation*—The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, should be obtained with the knowledge or consent of the individual.

2. *Purpose specification*—The purpose for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes.

[2]Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,972 (July 9, 1975).

3. *Use limitation*—Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.

4. *Data quality*—Personal information should be relevant to the purpose for which it is collected, and be accurate, complete, and current as needed for that purpose.

5. *Security safeguards*—Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.

6. *Openness*—The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.

7. *Individual participation*—Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.

8. *Accountability*—Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Striking that balance varies among countries and among types of information (e.g., medical versus employment information). TSA plans state that the Office of National Risk Assessment will design CAPPS II "to ensure that the highest level of [F]air [I]nformation [P]ractices are complied with while allowing [it] to achieve its mission of protecting the U.S. transportation systems and the public from potential foreign terrorists."

When viewed in this larger context, TSA's plans reflect actions to address each of these practices to at least some extent. For example, consistent with the *collection limitation* practice, TSA plans to not collect passengers' social security numbers from commercial data providers and to destroy most passenger information shortly after the completion of the travel itinerary. In addition, TSA plans to prohibit commercial data providers from using the information they receive from TSA for

commercial purposes appear consistent with the *use limitation* practice. Such a prohibition helps prevent the use of personal information in new ways unless required by law or with the consent of the individual.

However, to meet its evolving mission goals, TSA plans also appear to limit the application of certain of these practices. For example, TSA plans to exempt CAPPS II from the Privacy Act's requirements to maintain only that information about an individual that is relevant and necessary to accomplish a proper agency purpose. These plans reflect the subordination of the *use limitation* and *data quality* practices to other goals and raise concerns that TSA may collect and maintain more information than is needed for the purpose of CAPPS II and perhaps use this information for new purposes in the future. Further, TSA plans to limit the application of the *individual participation* practice by prohibiting passenger access to all personal information about them maintained in the CAPPS II system This raises concerns that inaccurate personal information will remain uncorrected in and continue to be accessed by CAPPS II. Because CAPPS II is still evolving, the extent to which the objectives of each practice are fulfilled may change as the program develops.

Such actions to limit the application of the Fair Information Practices do not violate federal requirements. Rather, they reflect TSA's efforts to balance privacy with other public policy interests associated with the mission goals of CAPPS II. TSA, however, has provided little explanation of how they have determined that CAPPS II will ensure the highest level of compliance with the Fair Information Practices possible. Further, TSA has not provided its rationale for other significant plans including exempting CAPPS II from certain Privacy Act requirements. The absence of such explanations of these balancing decisions raise privacy concerns. As the program evolves, it will ultimately be up to policymakers to determine if TSA has struck an appropriate balance between protecting personal privacy and other public policy interests.

Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 4, 2004

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

Dear Ms. Berrick

Thank you for the opportunity to comment on your draft report entitled, "Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges," GAO-04-385. We value the General Accounting Office's (GAO) continued interest in this vital program and desire to see this undertaking successfully completed.

The Department of Homeland Security appreciates the work done in this report to evaluate various aspects of Computer-Assisted Passenger Prescreening System II's (CAPPS II) development. We generally concur with the report and its recommendations and appreciate the very thorough discussion of CAPPS II development issues and challenges contained in the report. However, there are a number of areas within the report about which the Department would like to comment.

First, CAPPS II is a program still under development. As a result, we are not yet, nor could we be, at the point of having completely addressed many of the areas of concern identified by Congress in the Department of Homeland Security Appropriations Act, 2004.[1] We believe that while your report does discuss many of these issues and much of our progress in great detail, the results in brief and summary charts, which convey overall tone of the report, do not characterize our progress accurately. As of this date, CAPPS II does exist as a fully integrated, baseline functioning system. It has undergone integration testing (i.e., receiving data through the "Airline Data Interface," or "ADI," developed for CAPPS II). In its present state, CAPPS II is capable of receiving data through the ADI, cleansing and formatting the data, transmitting the formatted data through the identity authentication process, receiving an authentication score, performing a risk assessment, and generating a final risk assessment score. Overarching Privacy policies and a broad outline for redress mechanisms are in place, both within TSA and with the Chief Privacy

[1] Department of Homeland Security Appropriations Act, 2004, Pub.L. 108-90, section 519.

www.dhs.gov

Officer. However, because we are not currently authorized to receive Passenger Name Record (PNR) data for additional testing, we are not able to advance the program beyond the current state of development.

Second, the report focuses on international issues as an impediment to deployment, but does not clearly convey the complexity of the situation. The reality is that the European Commission and community are engaged in exactly the same struggle we are regarding how to balance the need for additional security in a post-9/11 era with the important principles of respect for individual rights and liberties, including privacy, on which our nation was founded. While the EU's legal framework may result in slightly different implementation of similar principles, the European forces and voices of law enforcement, counter terrorism, and public advocacy are seeking to achieve a similar balance on this issue for the European Union (EU). Thus, the perception of the EU's position in this area must be viewed in this larger context.

Third, we are concerned that the report does not adequately convey the degree of international cooperation we have achieved in the development of passenger screening mechanisms. For example, a number of countries have embraced the necessity of passenger screening--in fact, there are a number of countries that already have significant passenger screening programs in place. Further, the EU, while wary of the program, has engaged in a substantial and time-consuming negotiation with the Department in order to forge an agreement that is acceptable both under the aviation security act and the EU's data protection directive. This shows a willingness to work with us on these important issues and recognition of the fact that greater international cooperation is necessary to combat terrorism.

Most significantly, the Report does not acknowledge that the December 16, 2003 European Commission recommendation of adequacy provides that CAPPS II may use data collected by CBP under the adequacy agreement for testing. While this agreement must still be approved by appropriate European Parliamentary bodies, the agreement in principle highlights European recognition of the need to test the CAPPS II program to determine its viability, as well as its impact on personal privacy.

Finally, it is not accurate to state that the potential use of CAPPS II to detect individuals who are subject to federal or state outstanding warrants for crimes of violence or individuals with potential visa violations is an expansion of the program. As you are aware, the initial Privacy Act notice for the program, which was published in January 2003, announced the use of the system to detect any type of civil or criminal activity – it was neither limited to a particular class of violations, nor did it articulate that an outstanding warrant for prospective or suspected criminal or civil activity would be a necessary criteria for identification of risk. The Privacy Act notice published in August 2003, by clearly stating the categories of use (to detect terrorists and their affiliates or outstanding warrants for state or federal crimes of violence, or potential use in the future to detect visa violations), marked greater citizen protection by further delineating and limiting the categories of use than the initial Privacy Act notice.

Again, we sincerely appreciate your review of the program and commend you for the thorough analysis and discussion which comprises the meat of the report. The Department of Homeland Security looks forward to building on efforts already underway

to create an effective CAPPS II. We will continue to be cognizant of the concerns raised by Congress and public advocacy groups that are echoed in the draft GAO report, and will continue to work to address these concerns before the system becomes operational.

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

Sincerely,

Janet Hale
Under Secretary for Management

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen A. Berrick (202) 512-3404
David A. Powner (202) 512-9286
John R. Schulze (202) 512-4390

Staff Acknowledgments

In addition to the above, J. Michael Bollinger, Katherine Davis, Adam Hoffman, David Hooper, Wyatt R. Hundrup, Linda Koontz, Thomas Lombardi, Jan Montgomery, Colleen Phillips, David Plocher, Theresa Roberson, Karl Seifert, Al Stapleton, and Eric Winter made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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