



Testimony

Before the Subcommittee on Aviation,
Committee on Transportation and
Infrastructure, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, March 17, 2004

AVIATION SECURITY

Challenges Delay
Implementation of
Computer-Assisted
Passenger Prescreening
System

Statement of Norman J. Rabkin, Managing Director,
Homeland Security and Justice Issues and
David A. Powner, Director, Information Technology Issues





Highlights of GAO-04-504T, a testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives

AVIATION SECURITY

Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System

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 such effort 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 summarize the results of its previous report that looked at (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) additional challenges that could impede the successful implementation of the system.

What GAO Recommends

In a recent report (GAO-04-385), GAO recommended that the Secretary of the Department of Homeland Security (DHS) develop project plans, including schedules and estimated costs; a plan for completing critical security activities; a risk mitigation strategy for system testing; policies governing program oversight; and a process by which passengers can correct erroneous information. DHS generally concurred with the report and its recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-504T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkinn@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 completely 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. See table below for a summary of TSA's status in addressing the eight key legislative issues.

Status of TSA in Addressing Key Legislative 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 resolved		✓
Abuse prevention		✓	Redress process		✓

Source: GAO

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.

Mr. Chairman and Members of the Subcommittee:

The security of our nation's commercial aviation system has been a long-standing concern. For over 30 years, numerous efforts have been undertaken to improve aviation security, but weaknesses persist. Following the tragic events of September 11, 2001, substantial changes were made to strengthen aviation security and reduce opportunities for terrorists to hijack or destroy commercial aircraft. However, as recent flight cancellations over the last 3 months 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.

My testimony today focuses on the development of and challenges facing one particular effort underway to strengthen aviation security—the new Computer-Assisted Passenger Prescreening System (CAPPS II). More specifically, my testimony highlights three key areas: (1) the development status and plans for CAPPS II, (2) the status of CAPPS II in addressing eight program issues of particular concern to the Congress, and (3) additional challenges that pose major risks to the development and implementation of the system. My testimony is based on our recently issued report¹ and, because the development of CAPPS II is ongoing, updated information we have acquired since our report's issuance.

In summary, we found that:

- Key activities in the development of CAPPS II have been delayed, and the Department of Homeland Security's (DHS) Transportation Security Administration (TSA)—the agency responsible for developing CAPPS II—has not yet completed important system planning activities. TSA is currently behind schedule in testing and developing the initial phases—called increments—of CAPPS II due in large part to delays in obtaining needed passenger data for testing from air carriers because of privacy concerns. Furthermore, the system's initial operating capability—the point at which the system will be ready to operate with data from one airline—has been postponed and a new date has not been determined. TSA also has not yet established a complete plan that identifies specific system

¹U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, [GAO-04-385](#) (Washington, D.C.: Feb. 12, 2004).

functions that it will deliver, 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.

- TSA has not fully addressed seven of 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. The one issue that has been addressed involves the establishment of an internal oversight board to review the development of major systems, including CAPPs II. DHS and TSA are taking steps to address the remaining seven issues; however, they have not yet
 1. determined and verified the accuracy of the databases to be used by CAPPs II,
 2. stress tested and demonstrated the accuracy and effectiveness of all search tools to be used by CAPPs II,
 3. developed sufficient operational safeguards to reduce the opportunities for abuse,
 4. established substantial security measures to protect CAPPs II from unauthorized access by hackers and other intruders,
 5. adopted policies to establish effective oversight of the use and operation of the system,
 6. identified and addressed all privacy concerns, and
 7. developed and documented a process under which passengers impacted by CAPPs II can appeal decisions and correct erroneous information.
- In addition to facing developmental and operational 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.

Background

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 a flight. As the volume of passengers requiring screening increased and an awareness of terrorists' threats against the United States developed, a computerized system was implemented in 1998 to help identify passengers posing the greatest risk to a flight so that they could receive additional security attention. This system, known as CAPPs,² is operated by air carriers in conjunction with their reservation systems. CAPPs enables air carriers to separate passengers into two categories: those who require additional security screening—termed “selectees”—and those who do not. Certain information contained in the passenger's reservation is used by the system to perform an analysis against established rules and a government supplied “watch list” that contains the names of known or suspected terrorists. If the person is deemed to be a “selectee,” the boarding pass is encoded to indicate that additional security measures are required at the screening checkpoint. This system is currently used by most U.S. air carriers to prescreen passengers and prescreens an estimated 99 percent of passengers on domestic flights. For those passengers not prescreened by the system, certain air carriers manually prescreen their passengers using CAPPs criteria and the watch list.

Following the events of September 11, 2001, Congress passed the Aviation and Transportation Security Act³ requiring that a computer-assisted passenger prescreening system be used to evaluate all passengers, TSA's Office of National Risk Assessment has undertaken the development of a second-generation computer-assisted passenger prescreening system, known as CAPPs II. Unlike the current system that is operated by the air carriers, the government will operate CAPPs II. 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.

TSA program officials expect that CAPPs II will provide significant improvements over the existing system. First, they believe a centralized CAPPs II that will be owned and operated by the federal government will allow for more effective and efficient use of up-to-date intelligence

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

³Pub. L. No. 107-71, § 136, 115 Stat. 597, 637 (2001).

information and make CAPPS II more capable of being modified in response to changing threats. Second, they also believe that CAPPS II will improve identity authentication and reduce the number of passengers who are falsely identified as needing additional security screening. Third, CAPPS II is expected to prescreen all passengers on flights either originating in or destined for the United States. Last, an additional expected benefit of the system is its ability to aggregate risk scores to identify higher-risk flights, airports, or geographic regions that may warrant additional aviation security measures.

System 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. TSA plans to develop CAPPS II in nine increments, with each increment providing increased functionality. (See app. I for a description of these increments.) As each increment is completed, TSA plans to conduct tests that would ensure the system meets the objectives of that increment before proceeding to the next increment. The development of CAPPS II began in March 2003 with increments 1 and 2 being completed in August and October 2003, respectively. However, TSA has not completely tested these initial two increments because it was unable to obtain the necessary passenger data for testing from air carriers. Air carriers have been reluctant to provide passenger data due to privacy concerns. Instead, the agency deferred completing these tests until increment 3.

TSA is currently developing increment 3. However, due to the unavailability of passenger data needed for testing, TSA has delayed the completion of this increment from October 2003 until at least the latter part of this month 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 of the system in a simulated test environment that is not actively connected to an airline reservation system. Officials also said 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 implementation of the system 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

app. II for a timeline showing the original and revised schedule for CAPPS II increments.)

Further, we found that 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.⁴

TSA established plans for the initial increments of the system, including requirements for increments 1 and 2 and costs and schedules for increments 1 through 4. However, officials lack a comprehensive 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. Project officials also said 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 scheduled 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.

⁴U.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

In reviewing CAPPS II, we found that 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 issues⁵ that TSA must fully address before the system is deployed or implemented. These eight issues are

- establishing an internal oversight board,
- assessing the accuracy of databases,
- testing the system load capacity (stress testing) and demonstrating its efficacy and accuracy,
- installing operational safeguards to protect the system from abuse,
- installing security measures to protect the system from unauthorized access,
- establishing effective oversight of the system's use and operations,
- addressing all privacy concerns, and
- creating a redress process for passengers to correct erroneous information.

While TSA is in various stages of progress to address each of these issues, only the establishment of an internal oversight board to review the development of CAPPs II has been fully addressed. For the remaining issues, TSA program officials contend that their ongoing efforts will ultimately address each issue. However, due to system development delays, uncertainties regarding when passenger data will be obtained to test the system, and the need to finalize key policy decisions, officials were unable to identify a time frame for when all remaining issues will be fully addressed.

The following briefly summarizes the status of TSA's efforts to address each of the eight issues.

⁵Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003).

-
- Establishment of a CAPPs II oversight board has occurred.

DHS created an oversight board—the Investment Review Board—to review the department’s largest capital asset programs. The Board reviewed CAPPs II in October 2003. Based on this review, the Board authorized TSA to proceed with the system’s development. However, DHA noted some areas that the program needed to address. These areas included addressing 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 increment.

Although DHS has the Board in place to provide internal oversight and monitoring for CAPPs II and other large capital investments, we recently reported that concerns exist regarding the timeliness of its future reviews. DHS officials acknowledged that the Board is having difficulty reviewing all of the critical departmental programs in a timely manner.⁶ As of January 2004, DHS had identified about 50 of the largest capital assets that would be subject to the Board’s review. As CAPPs II’s development proceeds, it will be important for the Board to oversee the program on a regular and thorough basis to provide needed oversight.

In addition, on February 12, 2004, DHS announced its intentions to establish an external review board specifically for CAPPs II. This review board will be responsible for ensuring that (1) the privacy notice is being followed, (2) the appeal process is working effectively, and (3) the passenger information used by CAPPs II is adequately protected. However, in announcing the establishment of this review board, DHS did not set a date as to when the board will be activated or who would serve on the board.

- The accuracy of CAPPs II databases has not yet been determined.

TSA has not yet determined the accuracy—or conversely, the error rate—of commercial and government databases that will be used by CAPPs II. Since consistent and compatible information on database accuracy is not available, TSA officials said that they will be developing and conducting their own tests to assess the overall accuracy of information contained in

⁶U.S. General Accounting Office, *Information Technology: OMB and Department of Homeland Security Investment Reviews* [GAO-04-323](#) (Washington, D.C.: Feb. 10, 2004).

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.

In addition to testing the accuracy of commercial databases, TSA plans to better ensure the accuracy of information derived from 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. However, how to better ensure the accuracy of government databases will be more challenging. 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. A senior program official said that using data without assessing accuracy and mitigating data errors could result in erroneous passenger assessments; consequently government database accuracy and mitigation measures will have to be developed and completed before the system is placed in operation.

In mitigating errors in commercial and government databases, TSA plans to use 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.

- Stress testing and demonstration of the system's efficacy and accuracy have been delayed.

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. 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 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

Further, as the system is more fully developed, TSA will need to conduct 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 has 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 said 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.

TSA's attempts to obtain test data are still ongoing, and privacy issues remain a stumbling block. TSA officials 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 said that before the system is implemented, a final Privacy Act notice will be published. According to DHS's Chief Privacy Officer, the agency anticipated that the Privacy Act

notice would be finalized in March 2004. However, this official told us that the agency will not publish the final Privacy Act notice until all 15,000 comments received in response to the August 2003 Privacy Act notice are reviewed and testing results are available. DHS could not provide us a date as to when this will be accomplished. Further, 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, since we issued our report last month, a TSA official said 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.⁷

Due to schedule delays and the early stage of CAPPs II development, TSA has not implemented critical elements of an information system security program to reduce opportunities for abuse and protect against unauthorized access by hackers. These elements—a security policy, a system security plan, a security risk assessment, and the certification and accreditation of the security of the system—together provide a strong security framework for protecting information technology data and assets. While TSA has begun to implement critical elements of an information security management program for CAPPs II, these elements have not been completed. Until a specific security policy for CAPPs II is completed, TSA officials reported that they are using relevant portions of the agency's information security policy and other government security directives as the basis for its security policy. As for the system security plan, it is currently in draft. TSA expects to complete this plan by the time initial operating capability is achieved. Regarding the security risk assessment, TSA has postponed conducting this assessment because of development delays and it has not been rescheduled. The completion date remains uncertain because TSA does not have a date for achieving initial operating capability as a result of other CAPPs II development delays. As for final

⁷Because operational safeguards to reduce opportunities for abuse and security measures to protect CAPPs II from unauthorized access by hackers are so closely related, these two issues are discussed jointly.

certification and accreditation, TSA is unable to schedule the final certification and accreditation of CAPPs II because of the uncertainty regarding the system's development schedule.

The establishment of a security policy and 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.

TSA has not yet fully established controls to oversee the effective use and operation of CAPPs II. However, 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 goals and measures to assess the CAPPs II program's performance in meeting its objectives as required by the Government Performance and Results Act.⁸ Specifically, the agency has established five strategic objectives with preliminary performance goals and measures for CAPPs II. While this is a good first step, these measures may not be sufficient to provide the objective data needed to conduct appropriate oversight. TSA officials said that they are working with five universities to assess system effectiveness and management and will develop metrics to be used to measure the 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 or documented additional oversight controls to ensure that operations are effectively monitored and evaluated. Although TSA has built capabilities into CAPPs II to monitor and evaluate the system's operation and plans to conduct audits of the system to determine whether it is functioning as intended, TSA has not written all of the rules that will govern how the system will operate.

⁸Pub. L. No. 103-62, 107 Stat. 285 (1993).

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. 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's plans address privacy protection, but issues remain unresolved.

TSA's plans for CAPPS II reflect an effort to protect individual privacy rights, but certain issues remain unresolved. Specifically, TSA plans address many of the requirements of the Privacy Act, the primary legislation that regulates the government's use of personal information.⁹ For example, in January 2003, TSA issued a notice in the Federal Register that generally describes the Privacy Act system of records¹⁰ 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 guidance¹¹ 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, the public lacks assurance that the system will fully comply with the Privacy Act.

⁹Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

¹⁰Under 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.

¹¹Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,972 (July 9, 1975).

When viewed in the larger context of Fair Information Practices¹²—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. 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. 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.

- Redress process is being developed, but significant challenges remain.

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, TSA has not yet finalized this process. According to TSA officials, the redress process will make use of TSA’s existing complaint process—currently used for complaints from passengers denied boarding passes—to document complaints and provide these to TSA’s Ombudsman.¹³ Complaints relating to CAPPS II will be

¹²We refer to 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.

¹³The Ombudsman is the designated point of contact for TSA-related inquiries from the public.

routed through the Ombudsman to a Passenger Advocate—a position to be established within TSA for assisting individuals with CAPPs II-related concerns—who will help identify errors that may have caused a person to be identified as a false positive.¹⁴ If the passengers are not satisfied with the response received from the Passenger Advocate regarding the complaint, they will have the opportunity to appeal their case to the DHS Privacy Office.

A number of key policy issues associated with the redress process, however, still need to be resolved. These issues involve data retention, access, and correction. Current plans for data retention 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 has also not yet determined the extent of data access that will be permitted for those passengers who file a complaint. TSA officials said 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. Furthermore, TSA has not yet determined how the process of correcting erroneous information will work in practice. TSA documents and program officials said that it may be difficult for the Passenger Advocate to identify errors, and that it could be the passenger's responsibility to correct errors in commercial databases at their source.

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 said that available remedies for all persons seeking redress will be more fully detailed in CAPPs II's privacy policy,

¹⁴Passengers who are erroneously delayed or prohibited from boarding their scheduled flights are considered false positives.

which will be published before the system achieves initial operating capability.

Other Challenges Could Affect the Successful Implementation of CAPPS II

In addition to facing developmental and operational challenges related to key areas of interest to the Congress, CAPPS II 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 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.

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. However, obtaining international cooperation for access to these 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.

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. 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 said that it would discuss the use of European Union citizen passenger data in a second, later round of discussions.

Expansion of Mission

Our review found that CAPPS II may be expanded beyond its original purpose and 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. However, in the August 2003 interim final Privacy Act notice for CAPPs II, TSA stated that the system would seek to identify both domestic and foreign terrorists 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 and 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 have said that such changes are not an expansion of the system's mission because they believe it will improve aviation security and is consistent with CAPPs II's mission. However, program officials and advocacy groups expressed concern that focusing on persons with outstanding warrants, and possibly immigration violators, could put TSA at risk of diverting attention from the program's fundamental purpose. Expanding CAPPs II's 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 costs of passenger screening, as well as the number of passengers erroneously identified as needing additional security attention because some of the databases that could be used to identify wanted felons have reliability concerns.

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. TSA officials said 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. TSA officials said 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 in the databases used by CAPPs II. Additionally, officials said that data on identity theft may be available through credit bureaus and that in the future they expect to work with the credit bureaus to obtain such data. However, the officials 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 said that there should not be an expectation that CAPPS II will be 100 percent accurate in identifying all cases of identity theft. Further, the officials 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.

Concluding Observations

The events of September 11, 2001, and the ongoing threat of commercial aircraft hijackings as a means of terrorist attack against the United States continue to highlight the importance of a proactive approach to effectively prescreening airline passengers. An effective prescreening system would not only expedite the screening of passengers, 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 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, only one has been fully addressed. Additionally, concerns about mission expansion and identity theft add to the public's uncertainty about the success of CAPPS II.

Our recent report on CAPPS II made seven specific recommendations that we believe will help address these concerns and challenges. The development of plans identifying the specific functionality that will be delivered during each increment of CAPPS II and its associated milestones for completion and the expected costs for each increment would provide TSA with critical guidelines for maintaining the project's focus and achieving intended system results and milestones within budget. Furthermore, a schedule for critical security activities, a strategy for mitigating the high risk associated with system and database testing, and appropriate oversight mechanisms would enhance assurance that the

system and its data will be adequately protected from misuse. In addition to these steps, development of results-oriented performance goals and measures would help ensure that the system is operating as intended. Last, given the concerns regarding the protection of passenger data, the system cannot be fully accepted if it lacks a redress process for those who believe they are erroneously identified as an unknown or unacceptable risk.

Our recently published report highlighted each of these concerns and challenges and contained several recommendations to address them. DHS generally concurred with our findings and has agreed to address the related recommendations. By adequately addressing these recommendations, we believe DHS increases the likelihood of successfully implementing this program. In the interim, it is crucial that the Congress maintain vigilant oversight of DHS to see that these concerns and challenges are addressed.

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

GAO Contacts and Acknowledgments

For further information on this testimony, please contact Norman J. Rabkin at (202) 512-8777 or David A. Powner on (202) 512-9286. Individuals making key contributions to this testimony include J. Michael Bollinger, Adam Hoffman, and John R. Schulze.

Appendix I: CAPPS II Developmental Increments

The following describes general areas of functionality to be completed during each of the currently planned nine developmental increments of the Computer –Assisted Passenger Prescreening System (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 the completion of 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

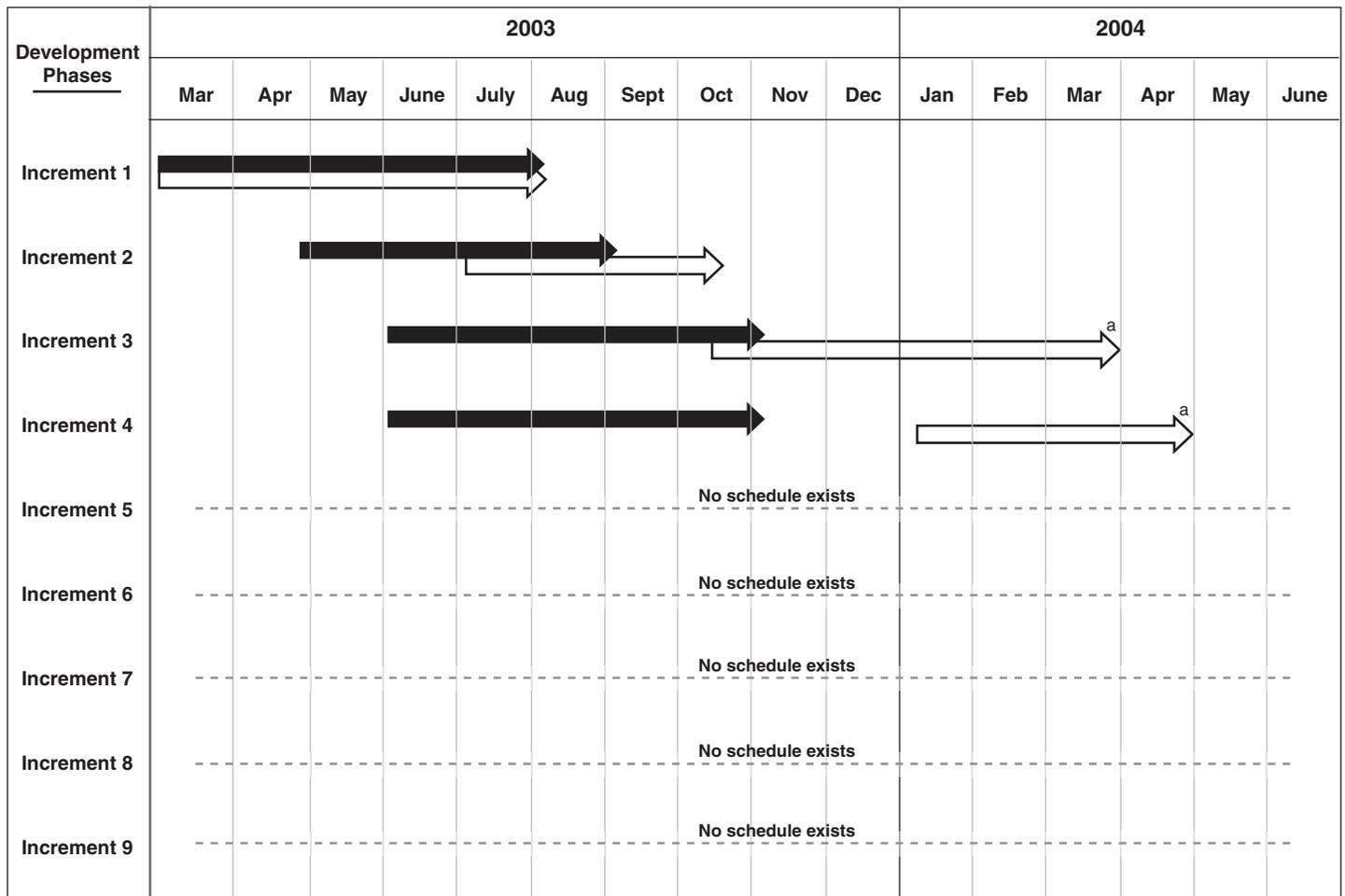
commercial data sources in the instance that little information on a passenger is available from original commercial data source.

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.

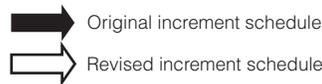
Increment 8. Enhanced risk assessments. This increment provides for the installation of capabilities and data sources to enhance risk assessments, which will lower the number of passengers falsely identified for additional screening. This increment also provides for a direct link to the checkpoint for 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 II: Timeline for Developing CAPPS II, by Original and Revised Increment Schedule



Source: GAO.



^aSystem functionality to be achieved at revised schedule dates will be less than originally planned.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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