United States Government Accountability Office

GAO

Report to Congressional Committees

March 2005

AVIATION SECURITY

Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-05-356, a report to congressional committees

March 2005

AVIATION SECURITY

Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed

Why GAO Did This Study

Among its efforts to strengthen aviation security, the Transportation Security Administration (TSA) is developing a new passenger prescreening system—known as Secure Flight. As required by Congress, TSA is planning to assume, through Secure Flight, the prescreening function currently performed by the air carriers. This report assesses the (1) status of Secure Flight's development and implementation, (2) factors that could influence the effectiveness of Secure Flight, (3) processes used to oversee and manage the Secure Flight program, and (4) efforts taken to minimize the impacts on passengers and protect passenger rights. In conducting this assessment, we addressed the 10 specific areas of congressional interest related to Secure Flight outlined in Public Law 108-334.

What GAO Recommends

GAO recommends that the Department of Homeland Security (DHS) direct TSA to take several actions to mange risks associated with Secure Flight's development, including (1) finalizing requirements and test plans, privacy and redress requirements, and program cost estimates; and (2) establishing plans to achieve connectivity to obtain data, and performance goals and measures. DHS generally concurred with GAO's findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-356.

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

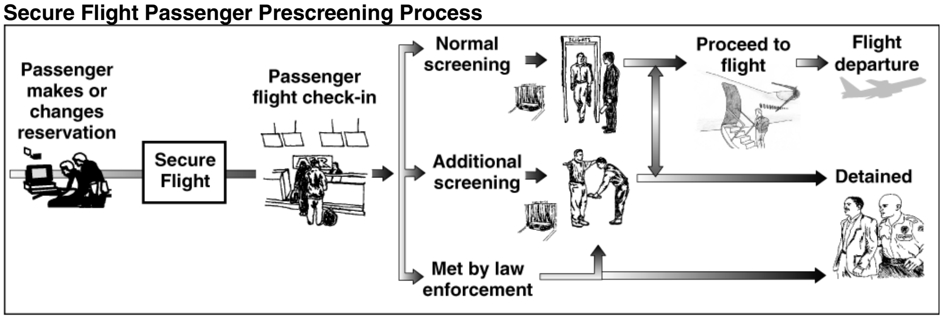
What GAO Found

TSA is making progress in addressing each of the key areas of congressional interest related to the development and implementation of Secure Flight, including developing and testing the system. However, TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the system's development. For example, while TSA has drafted a concept of operations and system requirements, it has not finalized these key documents or completed test activities that will need to be accomplished before Secure Flight becomes operational. Until requirements are defined, operating policies are finalized, and testing is completed—scheduled for later in the system's development—we cannot determine whether Secure Flight will fully address these areas of interest.

TSA also initiated a number of actions designed to improve the ability of Secure Flight to identify passengers who should undergo additional security scrutiny, in place of the prescreening currently conducted by air carriers. Specifically, TSA officials stated that recently completed initial testing identified improvements over the current prescreening system, and TSA plans to use intelligence analysts to increase the accuracy of data matches. However, the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny has not been fully determined. For example, TSA has not resolved how passenger data will be transmitted from air carriers to TSA to support Secure Flight operations. Further, the ability of Secure Flight to make accurate matches between passenger data and data contained in the terrorist screening database is dependent on the quality of the data used, which has not been determined.

TSA has also strengthened the oversight and management of Secure Flight, and has established relationships with key program stakeholders. However, air carriers expressed concerns regarding the uncertainty of system requirements, and the impact these requirements may have on the airline industry in terms of system modifications and costs. Additionally, TSA has taken steps to minimize potential impacts on passengers and to protect passenger rights during Secure Flight testing. However, TSA has not yet clearly defined the privacy impacts of the operational system or all of the actions TSA plans to take to mitigate potential impacts.

Secure Flight Passenger Prescreening Process



Source: GAO analysis of TSA data.

Contents

Tables

Figures

Abbreviations

CAPPS I	Computer-Assisted Passenger Prescreening System I
CAPPS II	Computer-Assisted Passenger Prescreening System II
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
OMB	Office of Management and Budget
PNR	Passenger name record
TSA	Transportation Security Administration
TSC	Terrorist Screening Center

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 28, 2005

Congressional Committees:

Strengthening the security of commercial aviation has been a goal—and a challenge—for many years, but since the September 11, 2001, terrorist attacks, it has become a much more critical issue. The attacks demonstrated that the consequences of inadequate security can be more severe and tragic than previously imagined. Moreover, the attacks showed that terrorists are targeting commercial aviation within the nation's borders, and that measures taken to provide security were not always effective. Consequently, since that time, the federal government has initiated a number of efforts designed to strengthen the security of virtually all aspects of commercial aviation.

Efforts to strengthen aviation security cover many areas, including improved controls over screening passengers and baggage, and securing restricted airport areas and airport perimeters. A recent initiative to strengthen security is in the area of passenger prescreening. The prescreening of passengers—that is, identifying passengers that pose a security risk before they reach the passenger screening checkpoint—can enable officials to focus security efforts on those passengers representing the greatest potential threat. Since the late 1990s, passenger prescreening has been conducted using the Computer-Assisted Passenger Prescreening System (CAPPS I)—in which data related to a passenger's reservation and travel itinerary are compared against characteristics used to select passengers who require additional security scrutiny, known as CAPPS I rules—and through the matching of passenger names to terrorist watch lists. However, following the events of September 11, it became clear that the capabilities of the existing prescreening system to identify possible terrorists needed improvement. Consequently, in November 2001, Congress passed the Aviation and Transportation Security Act, which established the Transportation Security Administration (TSA) and directed that it assume most of the responsibilities for civil aviation security.[1] In accordance with the act's requirement that a computer-assisted passenger prescreening system be used to evaluate all passengers, TSA subsequently began an effort to develop a new prescreening system known as CAPPS II

[1] Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

that, unlike the current system that operates as part of each airline's reservation system, would be operated by TSA. Further, in July 2004, the National Commission on Terrorists Attacks upon the United States, also known as the 9/11 Commission, reported that the current passenger prescreening system needed improvements, and that the watch lists used by the air carriers did not include all terrorists or terrorism suspects because of concerns about sharing intelligence information with private firms and foreign countries. The commission recommended that passenger screening be performed by the federal government, and make use of the larger consolidated watch list database maintained by the government.[2]

Because of a variety of delays and challenges, in August 2004, the Department of Homeland Security (DHS) cancelled the development of CAPPS II. In its place, TSA announced that it would develop a new prescreening program, called Secure Flight, that would respond to the commission's recommendation by taking over the responsibility—from air carriers—for prescreening passengers, using the larger consolidated watch list database not currently available to air carriers. In developing Secure Flight, TSA plans to incorporate some but not all of the functionality planned for the CAPPS II program. Specifically, Secure Flight is being developed to compare passenger information against data from the consolidated watch list database. TSA is also considering incorporating CAPPS I rules processing as part of Secure Flight, and may include the use of commercial data (e.g., personally identifiable information that either identifies an individual or is directly attributed to an individual, such as name, address, and phone number) if the data can be shown, through testing, to add to the security benefits of Secure Flight.

Public Law 108-334, enacted in October 2004, mandated that we assess and report on 10 aspects of the development and implementation of Secure Flight.[3] This report satisfies the requirements of that mandate. Specifically, this report addresses the following questions: (1) What is the status of Secure Flight's development and implementation? (2) What factors could influence the effectiveness of Secure Flight? (3) What procedures have been put in place to oversee and manage the Secure Flight program, including ensuring stakeholder coordination? And (4) What efforts are

[2] The 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, July 2004.

[3] Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, § 522, 118 Stat. 1298, 1319-20 (2004).

being taken to minimize the impacts on passengers and protect passenger rights? In answering these questions, we addressed the 10 specific areas of congressional interest that we were mandated to review based on the current status of Secure Flight's development. These areas address the establishment of a redress process, assessment of the accuracy of databases and the effectiveness of Secure Flight, system stress testing, program oversight, operational safeguards, security measures, oversight policies governing the use and operation of the system, system privacy protections, system modifications to accommodate states with unique air transportation needs, and life-cycle cost estimates and expenditure plans. (See app. I, table 5, for a description of the 10 areas identified in Public Law 108-334 and the sections of the report in which they are addressed.) Since some of the information addressing the congressional areas of interest is considered Sensitive Security Information, we are also issuing a separate letter containing this information.[4]

To address these questions, we reviewed available Secure Flight program documentation to include system requirements, test plans, and privacy notices. We also interviewed officials from DHS, TSA, U.S. Customs and Border Protection (CBP), and the Terrorist Screening Center (TSC)[5] to discuss the status of the program's development as of March 2005, as well as its anticipated operations. Since TSA developed Secure Flight from a modified version of the CAPPS II program, and will incorporate program criteria from CAPPS I, we also reviewed relevant CAPPS II and CAPPS I program documentation. Further, we questioned officials from selected air carriers and interviewed personnel from several trade organizations and privacy advocacy organizations regarding issues related to Secure Flight's development and implementation. We conducted our work from April 2004 until March 2005 in accordance with generally accepted government auditing standards. A detailed discussion of our scope and methodology is contained in appendix I.

[4] GAO, *Aviation Security: TSA Modifications to Rules for Prescreening Passengers*, GAO-05-445SU (Washington, D.C.: Mar. 28, 2005).

[5] TSC was established in accordance with Homeland Security Presidential Directive/HSPD-6 to consolidate the government's approach to terrorism screening, including the use of terrorist information for screening purposes. TSC is an interagency effort involving DHS, Department of Justice, Department of State, and intelligence community representatives, and is administered by the Federal Bureau of Investigation. TSC maintains the terrorist screening database, which consolidates information from terrorist watch lists to provide government screeners with a unified set of antiterrorist information.

Results in Brief

Overall, TSA is making progress in addressing key areas of congressional interest related to the development and testing, system effectiveness, program management and oversight, and privacy protections for the Secure Flight program, as outlined in Public Law 108-334. Table 1 provides a summary of TSA's status in addressing each of the ten areas of congressional interest. However, TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the program's development. Specifically, initial tests have only recently been completed, and key policy decisions—including what data will be collected and how it will be transmitted—have not yet been made. Until requirements are fully defined, operating policies are finalized, and testing is completed—scheduled for later in the system's development—we cannot determine whether TSA will fully address these areas of interest.

Table 1: Summary of TSA's Status in Addressing Ten Areas of Congressional Interest Included in Public Law 108-334 as of March 15, 2005

Areas of congressional interest (short title and page number in report that further describes status)	TSA status in addressing area of congressional interest
Stress test system and demonstrate efficacy and accuracy (page 25)	Under way[a]
Assess accuracy of databases (page 27)	Under way
Modifications with respect to intrastate travel to accommodate states with unique air transportation needs (page 34, also see GAO-05-445SU)	Under way
Establish internal oversight board (page 39)	Addressed[b]
Establish effective oversight of system use and operation (page 43)	Under way
Install operational safeguards to protect system from abuse (page 48)	Under way
Install security measures to protect system from unauthorized access (page 48)	Under way
Life-cycle costs and expenditure plans (page 50)[c]	Under way
Address all privacy concerns (page 54)	Under way
Create redress process for passengers to correct erroneous information (page 56)	Under way

Source: GAO analysis.

[a] Under way indicates that TSA provided evidence that it has begun to address this issue.

[b] Addressed indicates that TSA provided evidence that it has addressed this issue.

[c] TSA officials stated that they plan to develop life-cycle cost estimates after system requirements have been defined, and that they recently finalized an expenditure plan.

TSA is making progress in the development and testing of Secure Flight and is attempting to build in more rigorous processes than those used for CAPPS II. Specifically, TSA has drafted a number of key documents to assist in providing program oversight, including a draft concept of operations, a draft requirements document, and a draft project schedule.

However, TSA has not yet finalized these documents. Further, although TSA uses a working milestone chart to coordinate its many activities, key milestones for the Secure Flight program have slipped. For example, the date when Secure Flight is expected to achieve initial operational capability with two air carriers slipped by about 4 months. TSA is also completing initial Secure Flight testing to determine data needs and system functions, which are basic to defining how Secure Flight will operate. However, key system testing including stress testing—to verify that the entire system will function as intended in an operational environment—has not been completed. Further, although TSA expects to complete stress testing prior to initial operational deployment, scheduled for August 2005, it has not yet designed the procedures it will use to conduct these tests. Until TSA finalizes key program documents and completes additional system testing, it is uncertain whether Secure Flight will perform as intended, and whether it will be ready for initial operational deployment by August 2005.

TSA has begun, or has plans to initiate, a number of actions designed to improve the ability of Secure Flight to identify passengers who should undergo additional security scrutiny, in place of prescreening currently conducted by air carriers. Specifically, TSA recently completed initial testing to identify those elements that will be used to match air carrier passenger data to data contained in the TSC's terrorist screening database, and the effectiveness of these data in making accurate matches. According to TSA officials, initial test results showed that the Secure Flight system was effective in matching PNR data with data contained in the terrorist screening database, and that data matching can be improved by adding additional information to PNR data, such as date of birth. However, because this testing has only recently been completed and test results have not been fully documented and analyzed, we were unable to independently assess these results. TSA also plans to use intelligence analysts to help resolve discrepancies in the matching of passenger data to data contained in the terrorist screening database. In addition, TSA recently modified the CAPPS I rules, which are currently being implemented and may also be used in Secure Flight, to facilitate more targeted screening of individuals. Although TSA is taking these actions, the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny has not been fully determined, and it can be affected by data quality and other factors. For example, TSA has not resolved how passenger data will be transmitted from air carriers to TSA to support Secure Flight operations. Further, the ability of Secure Flight to make accurate matches between passenger data and data contained in the terrorist screening database is dependent on the type and quality of the data. Although the TSC and TSA have taken, or plan to take, a number of actions to improve the quality of the data in the terrorist screening database, the accuracy of this data has not been fully determined. Another factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's ability to identify passengers who assume the identity of another individual by committing identity theft.

DHS and TSA have also taken steps to strengthen their oversight and management of Secure Flight, including coordinating with key stakeholders. However, a number of important issues will need to be resolved as program requirements are finalized and system testing is completed, and before Secure Flight becomes operational. DHS and TSA have provided oversight through a number of bodies designed to manage Secure Flight's development and implementation. TSA also reported strengthening its oversight of Secure Flight contractors through various methods, including increasing the number of TSA staff with contract oversight responsibilities. TSA officials also reached out to key external stakeholders, such as air carriers, whom they identified as integral to the successful implementation and operations of Secure Flight. These efforts should help DHS and TSA in managing its development and implementation efforts. Although DHS and TSA have taken these actions, however, TSA has not yet finalized oversight policies governing the use and operation of Secure Flight, or completed performance measures to measure program results. Further, although TSA has reached out to key external stakeholders who will be integral to Secure Flight operations, officials from these organizations expressed concerns regarding the uncertainty of Secure Flight system and data requirements, and the impact these requirements may have on the airline industry in terms of system modifications and costs. Data requirements and associated impacts on air carriers will need to be resolved before TSA can begin its initial operations with two air carriers in August 2005. TSA also has not finalized a security risk assessment and security plan, due largely to the early stage of the system's development. In addition, TSA did not develop life-cycle cost estimates and only recently completed an expenditure plan. Life-cycle cost estimates and expenditure plans are critical components of sound program management for the development of any major investment. Without fully developed plans addressing Secure Flight operations, security, and costs, individuals responsible for overseeing the program may not have the information needed to manage program risks and allocate resources.

Additionally, TSA has recognized that Secure Flight has the inherent potential to adversely affect the privacy rights of the traveling public because of the use of passenger data, and has begun to take steps to minimize potential impacts on passengers and to protect passenger rights during the testing phase of Secure Flight. However, TSA has not yet clearly defined the privacy impacts of Secure Flight in an operational environment, or all of the actions TSA plans to take to mitigate potential impacts. TSA also drafted a redress process to provide passengers who believe they were inappropriately delayed from boarding their scheduled flights because of Secure Flight a means by which to appeal these decisions and possibly correct erroneous data found in the terrorist screening database or in commercial databases, should TSA decide to use commercially available data. However, TSA has not yet clearly defined how it plans to implement its redress process for Secure Flight, such as how errors, if identified, will be corrected, particularly if commercial databases are used. In addition, although DHS and TSA have taken steps to address international privacy concerns in developing Secure Flight, such as limiting Secure Flight to prescreening only domestic passengers, issues remain, particularly with regard to the European Union. Specifically, TSA has acknowledged that the use of passenger data that originates in reservations made in a European Union country may create concerns under that country's privacy laws. Until TSA fully defines its operational plans for Secure Flight—which officials stated they plan to do later in the system's development—and addresses international privacy concerns, it will remain difficult to determine whether the planned system will offer reasonable privacy protections to passengers who are subject to prescreening or mitigate potential impacts on passengers' privacy.

To help manage risks associated with Secure Flight's continued development and implementation, and to assist TSA in developing a framework from which to support its efforts in addressing congressional areas of interest outlined in Public Law 108-334, we are making a number of recommendations to the Secretary of the Department of Homeland Security. These recommendations include finalizing requirements and test plans, developing a plan for transmitting data from and to air carriers to support Secure Flight operations, developing performance goals and measures and life-cycle costs, and finalizing policies and issuing associated documentation detailing privacy protections and a system of redress.

We provided a draft of this report to DHS for its review and comment. DHS, in its written comments, generally agreed with our findings and recommendations, and identified some actions it has initiated to implement the recommendations. For example, DHS stated that TSA plans to complete the Secure Flight concept of operations by March 2005, and system requirements by April 2005. DHS also noted that TSA is currently finalizing a redress process for passengers who feel they have been unfairly or incorrectly singled out for additional screening.

DHS also provided technical comments related to the program's development, testing, and implementation. These comments were incorporated as appropriate. A copy of DHS's comments is included in appendix II.

Background

The Transportation Security Administration is responsible for securing all modes of transportation while facilitating commerce and ensuring the freedom of movement for the traveling public. Passenger prescreening is one program among many that TSA uses to secure the aviation sector. The process of prescreening 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. Currently, U.S. air carriers conduct passenger prescreening using the Computer-Assisted Passenger Prescreening System, known as CAPPS I, and by comparing passenger names against government-supplied terrorist watch lists.

Current Passenger Prescreening

Passenger prescreening is used to identify passengers who may pose a higher risk to aviation security than other passengers and therefore should receive additional and more thorough security scrutiny. The current prescreening process consists of two components. First, after a passenger makes a reservation, the air carrier checks the passenger's reservation information contained in the air carrier's passenger name record (PNR)[6] against a set of established system rules, referred to as the CAPPS I rules.[7] Second, the air carrier checks the passenger's name against government-supplied watch lists that contain the names of individuals who, for certain

[6] The PNR contains data related to a passenger's reservation and travel itinerary and is contained in an air carrier's reservation system. Such data can include the passenger's name, phone number, number of bags, seat number, and form of payment, among other information.

[7] CAPPS I rules are characteristics that are used to select passengers who require additional security scrutiny.

reasons, are either not allowed to fly (the no-fly list) or pose a higher than normal risk and therefore require additional security attention (the selectee list). Passengers on the no-fly list are denied boarding passes and are not permitted to fly unless cleared by law enforcement officers. Passengers who are selected by the CAPPS I rules or who are on the selectee list are issued boarding passes, and they and their baggage undergo additional security measures. Approximately 99 percent of all passengers on domestic flights are screened under the air carrier-operated, automated CAPPS I system.[8]

CAPPS II

Following the events of September 11, and in accordance with the requirement set forth in the Aviation and Transportation Security Act that a computer-assisted passenger prescreening system be used to evaluate all passengers before they board an aircraft,[9] TSA established the Office of National Risk Assessment to develop and maintain a capability to prescreen passengers in an effort to protect U.S. transportation systems and the public against potential terrorists. In March 2003, this office began developing the second-generation computer-assisted passenger prescreening system, known as CAPPS II, to provide improvements over the current prescreening process, and to screen all passengers flying into, out of, and within the United States. Under the CAPPS II program, the responsibility and financial costs of passenger prescreening were to be transferred from the air carriers to the government. In addition, CAPPS II was to perform different analyses and access more diverse data, including data from government and commercial databases, to classify passengers according to their level of risk (i.e., acceptable risk, unknown risk, or unacceptable risk), which would in turn be used to determine the level of security screening each passenger would receive. Table 2 lists the specific capabilities that TSA planned to incorporate into CAPPS II, which the agency believed were needed to strengthen passenger prescreening.[10]

[8] The remaining 1 percent of passengers are manually screened by air carriers who do not have an automated system.

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

[10] TSA planned to incorporate eight capabilities into the CAPPS II program. We have only listed seven of these capabilities, because one is Sensitive Security Information.

Table 2: System Capabilities Planned for CAPPS II

Capability	Description
Watch list matching	Comparison of data contained in the passenger's reservation (PNR) with information contained in government watch lists (selectee and no-fly lists) to identify potential threats to aviation security and other individuals of interest to the counterterrorism community
CAPPS I rules application	Matching information in the PNR to CAPPS I rules to identify individuals who should be subject to additional security screening
Identity authentication	Checking PNR data against commercial databases to assist in confirming the passenger's identity
Criminal checks	Matching PNR data against lists of international fugitives and government "wanted lists" to identify known criminals
Intelligence-based search for unknown terrorists	Using algorithms developed through intelligence modeling to identify previously unknown terrorists by searching for patterns in an individual's travel or transaction history that are indicative of terrorist activities
Use of opt-in lists	Maintaining a list of individuals, who have been previously cleared under credentialing programs, such as registering passengers in advance of making reservations, to minimize the volume of passengers that must be prescreened
Use of alert lists	Providing the capability to create a temporary watch list based on information extracted from current intelligence reports, such as blocks of stolen passports

Source: TSA.

In February 2004, we reported—in response to a mandate in the fiscal year 2004 Department of Homeland Security Appropriation Act[11]—that TSA had not yet developed critical elements associated with sound project planning for CAPPS II, including a plan for the specific functionality to be delivered and the costs expected to be incurred throughout the system's development.[12] We also reported that TSA had not fully addressed seven of eight issues identified by Congress as key areas of interest related to the development and implementation of CAPPS II, such as privacy protection, passenger redress, and system security. Following our evaluation and congressional oversight hearings, DHS initiated an internal review of the CAPPS II program.

[11] The Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003), mandated that GAO review eight areas related to the development and implementation of CAPPS II, including system development and security, privacy, redress, and oversight.

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

Further, in July 2004, the National Commission on Terrorists Attacks upon the United States, commonly known as the 9/11 Commission, reported that the current air carrier-operated passenger prescreening system—CAPPS I and watch list matching—needed improvements, and that the watch lists used by the air carriers did not include all terrorists or terrorism suspects because of concerns about the government sharing intelligence information with private firms and foreign countries. The commission recommended that passenger prescreening be performed by the federal government and make use of the larger consolidated watch list database maintained by the government.[13] Taking into consideration the commission's recommendations and the results of DHS's internal review of CAPPS II, among other factors, TSA cancelled the development of CAPPS II in August 2004.

Secure Flight

Shortly after the CAPPS II program was cancelled, TSA announced that it planned to develop a new passenger prescreening program called Secure Flight. TSA plans to operate Secure Flight on the Transportation Vetting Platform—the development of which began under CAPPS II and includes the software for watch list matching and CAPPS I rules analysis.[14] According to TSA, Secure Flight will leverage the system development efforts already accomplished for CAPPS II, but will have several fundamental differences. Specifically, TSA is designing Secure Flight to incorporate only some of the capabilities planned for CAPPS II such as the core capabilities of watch list matching and CAPPS I rules application.[15] Secure Flight will also only prescreen passengers flying domestically within the United States, rather than passengers flying into and out of the United States. Table 3 provides a summary of the capabilities planned for

[13] *The 9/11 Commission Report.*

[14] TSA plans to use this centralized vetting capability to identify terrorist threats in support of various DHS and TSA programs. Further, TSA plans to use the platform to ensure that persons working at sensitive locations; serving in trusted positions with respect to the transportation infrastructure; or traveling as cockpit and cabin crew into, within, and out of the United States are properly screened depending on their activity within the transportation system. In addition to supporting the Secure Flight and Crew Vetting programs, TSA expects to leverage the platform with other applications such as TSA Screeners and Screener applicants, commercial truck drivers with Hazardous Materials Endorsements, aviation workers with access to secure areas of the airports, alien flight school candidates, and applicants for TSA's domestic Registered Traveler program.

[15] TSA planned to incorporate eight capabilities into the CAPPS II program. We have only listed seven of these capabilities, since one is Sensitive Security Information.

CAPPS II, as compared with the capabilities currently provided by the current passenger prescreening program and those planned for the Secure Flight program. As shown in table 3, TSA does not plan to add additional features beyond the current passenger prescreening program, with the exception of matching PNR data against an expanded terrorist watch list, which will be provided by the TSC. TSA is also exploring the feasibility of using commercial data as part of Secure Flight if the data are shown, through testing, to increase the effectiveness of the watch list matching feature. TSA does not currently plan for Secure Flight to include checking for criminals, performing intelligence-based searches, or using alert lists.[16] TSA has not yet determined whether Secure Flight will assume the application of CAPPS I rules from the air carriers, or if an opt-in list capability will be used as part of Secure Flight.[17]

[16] While TSA does not plan to include criminal checks within Secure Flight, it does plan to incorporate this capability into the platform, where it may be used by other vetting applications, such as Crew Vetting.

[17] An opt-in list could include passengers participating in TSA's Registered Traveler program, which is currently operating in the pilot phase at five airports. Under this program, frequent travelers at select airports are able to volunteer for the program. Volunteers are asked to submit information, including biometrics, necessary for TSA to determine eligibility. The biometric information, such as fingerprints, is used for identity verification purposes and, in conjunction with a security assessment, allows passengers at the pilot airport locations to go through an expedited security screening process. The results of the five-airport pilot program will determine future applications of the Registered Traveler concept at other airports.

Table 3: Key Capabilities for Passenger Prescreening Programs

	Capability included in program		
Capability	Current prescreening program	CAPPS II	Secure Flight
Watch list matching	✓	✓	✓[a]
CAPPS I rules application	✓	✓	To be determined[b]
Identity authentication		✓	To be determined[c]
Criminal checks		✓	
Intelligence-based search for unknown terrorists		✓	
Use of opt-in lists		✓	To be determined[d]
Use of alert lists		✓	

Source: GAO analysis of TSA information.

[a] Secure Flight will use an expanded watch list that includes more information than the current no-fly and selectee lists used by the air carriers.

[b] TSA has not yet determined whether air carriers will retain responsibility for applying the CAPPS I rules or whether this function will be preformed by TSA.

[c] TSA plans to make a decision on the use of commercial data for Secure Flight based on the results of current testing.

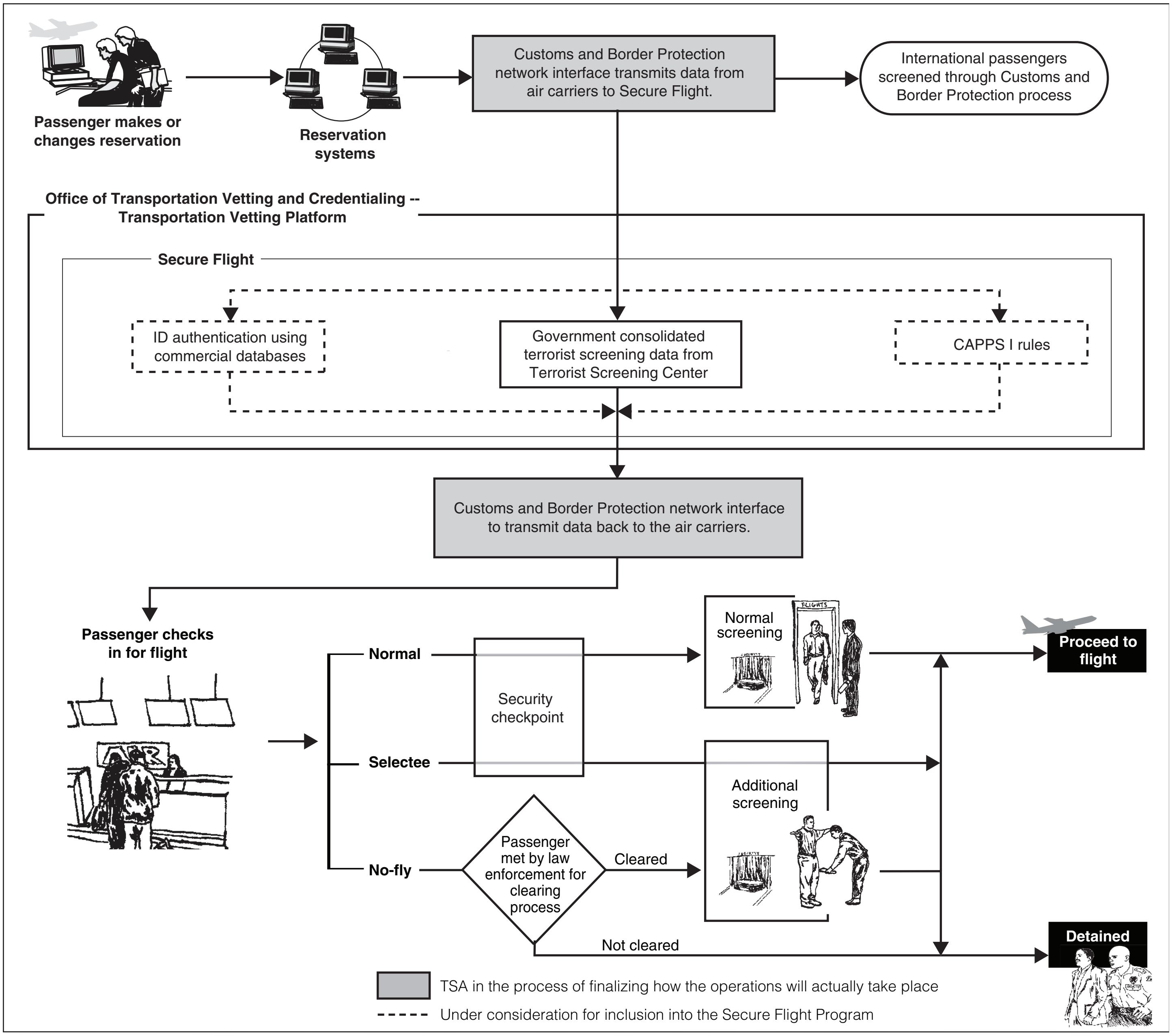
[d] TSA plans to examine whether Secure Flight will use an opt-in list, which could include those passengers participating in TSA's Registered Traveler program.

Secure Flight is currently undergoing development and testing, and policy decisions regarding the operations of the program have not been finalized.[18] However, TSA officials have described how they anticipate Secure Flight to operate, as illustrated in figure 1. When a passenger makes flight arrangements, the air carrier or reservation company will complete the reservation by entering PNR data in its reservation system, as is done currently. Once the reservation is completed, the PNR will be electronically stored by the air carriers. Approximately 72 hours prior to the flight, the PNR will be sent to Secure Flight through a network connection provided by DHS's CBP. Reservations that are made less than 72 hours prior to flight time will be sent immediately to TSA. Upon receipt of the PNR, TSA plans to process the PNR data through the Transportation Vetting Platform. During this process, Secure Flight will determine if the

[18] The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19, requires that TSA begin to assume responsibility for the passenger prescreening function within 180 days after the completion of testing.

data contained in the PNR match the data in the TSC terrorist screening database and potentially analyze the passenger's PNR data against the CAPPS I rules, should TSA decide to assume this responsibility from the air carriers. As noted earlier, TSA has not yet determined whether CAPPS I rules processing will be performed by TSA or by the air carriers. In order to match PNR data to information contained in the terrorist screening database, TSC plans to provide TSA with a subset of the database for use in Secure Flight, and provide updates as they occur. All individuals listed in the TSC data subset are to be classified as either selectees (will be required to undergo secondary screening before being permitted to board an aircraft) or no-flys (will be denied boarding unless they are cleared by law enforcement personnel). When Secure Flight completes its analysis, each passenger will be assigned one of three screening categories: normal screening required (no match against the terrorist screening database or CAPPS I rules), selectee (a match against the selectee list or the CAPPS I rules, or random selection), or no-fly (a match against the no-fly list). The results will be stored within the Secure Flight system until 24 hours prior to departure, at which time they will be returned to the air carriers.

Figure 1: Planned Operations of Secure Flight


Passenger makes or changes reservation
Reservation systems
Customs and Border Protection network interface transmits data from air carriers to Secure Flight.
International passengers screened through Customs and Border Protection process
Office of Transportation Vetting and Credentialing -- Transportation Vetting Platform
Secure Flight
ID authentication using commercial databases
Government consolidated terrorist screening data from Terrorist Screening Center
CAPPS I rules
Customs and Border Protection network interface to transmit data back to the air carriers.
Passenger checks in for flight
Normal
Selectee
No-fly
Security checkpoint
Normal screening
Additional screening
Passenger met by law enforcement for clearing process
Cleared
Not cleared
Proceed to flight
Detained
TSA in the process of finalizing how the operations will actually take place
Under consideration for inclusion into the Secure Flight Program

Source: GAO analysis of TSA data.

As shown in figure 1, when the passenger checks in for the flight at the airport, the passenger will receive a level of screening based on his or her designated category. A “normal screening” passenger will be provided a boarding pass and allowed to proceed to the screening checkpoint in the normal manner. A “selectee” passenger will receive a boarding pass but will undergo additional security scrutiny at the screening checkpoint. A “no-fly” passenger will not be issued a boarding pass. 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. TSA expects that all information specific to a PNR record will be purged from the Secure Flight temporary storage database 72 hours after completion of the itinerary, unless a redress action is initiated by the passenger. TSA plans to use the redress process to provide passengers who believe they were inappropriately delayed from boarding their scheduled flights because of Secure Flight a means by which to appeal these decisions.

After the completion of testing, TSA plans to make policy decisions regarding the scope and operation of Secure Flight, including the required PNR data to be obtained from air carriers and whether Secure Flight will use commercial data to enhance the watch list matching capability. TSA expects to begin initial operations of Secure Flight with two U.S. air carriers in August 2005 and systematically bring other U.S. air carriers online with Secure Flight in 2006. TSA estimates that Secure Flight will prescreen about 2 million domestic passengers per day when fully operational with all domestic air carriers. For fiscal year 2005, TSA was allocated $35 million for the development of Secure Flight. The President’s fiscal year 2006 budget request includes approximately $81 million for Secure Flight development and implementation.

To consolidate and strengthen TSA’s screening capability, in November 2004, DHS combined the Office of National Risk Assessment—which developed CAPPS II—with the Credentialing Program Office to become the Office of Transportation Vetting and Credentialing.[19] By merging these two offices, TSA expects to help provide assurance that Secure Flight and the various credentialing programs within DHS and TSA, which operate on the Transportation Vetting Platform, will be executed effectively. In addition, in an attempt to achieve greater synergy and avoid duplication of effort, DHS has proposed in its fiscal year 2006 budget request to create an

[19] The Credentialing Program Office was responsible for worker-screening programs, including aviation workers, alien flight students, and the Registered Traveler Program.

Office of Screening Coordination and Operations within DHS's Border and Transportation Security Directorate. The purpose of this office will be to coordinate a comprehensive approach to several ongoing terrorist-related screening initiatives—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure. If implemented, this office would absorb Secure Flight as well as additional DHS and TSA screening programs, including programs operating on the Transportation Vetting Platform.

Development and Testing of Secure Flight Are Under Way, but Key Activities Have Not Yet Been Completed

TSA is making progress in the development and testing of Secure Flight and is attempting to build in more rigorous processes than those used for CAPPS II. To accomplish these efforts, TSA has developed a draft concept of operations, a draft systems requirement document, and a draft project schedule to guide its activities. However, TSA has not yet finalized these documents. Further, although TSA is taking actions to more effectively manage the Secure Flight system's development, key milestones have slipped, including the date when Secure Flight is expected to begin initial operations with two air carriers, by about 4 months. TSA has acknowledged that meeting its Secure Flight schedule constitutes an area of risk.

Currently, TSA is completing testing to determine Secure Flight's data needs and system functions, which are basic to defining how Secure Flight will operate, and plans to complete important system testing activities such as end-to-end performance and stress testing the entire system.[20] According to TSA officials, TSA plans to finalize its concept of operations and system requirements prior to its final phase of testing the entire system, which is scheduled to begin in April 2005. Until TSA finalizes these documents and completes additional system testing, it is uncertain how well Secure Flight will perform or whether it will be ready for operational deployment by August 2005.

[20] End-to-end testing is conducted to verify that the entire system, including any external systems with which it interfaces, functions as intended in an operational environment. Stress testing refers to measuring a system's performance and availability in times of particularly heavy (i.e., peak) load.

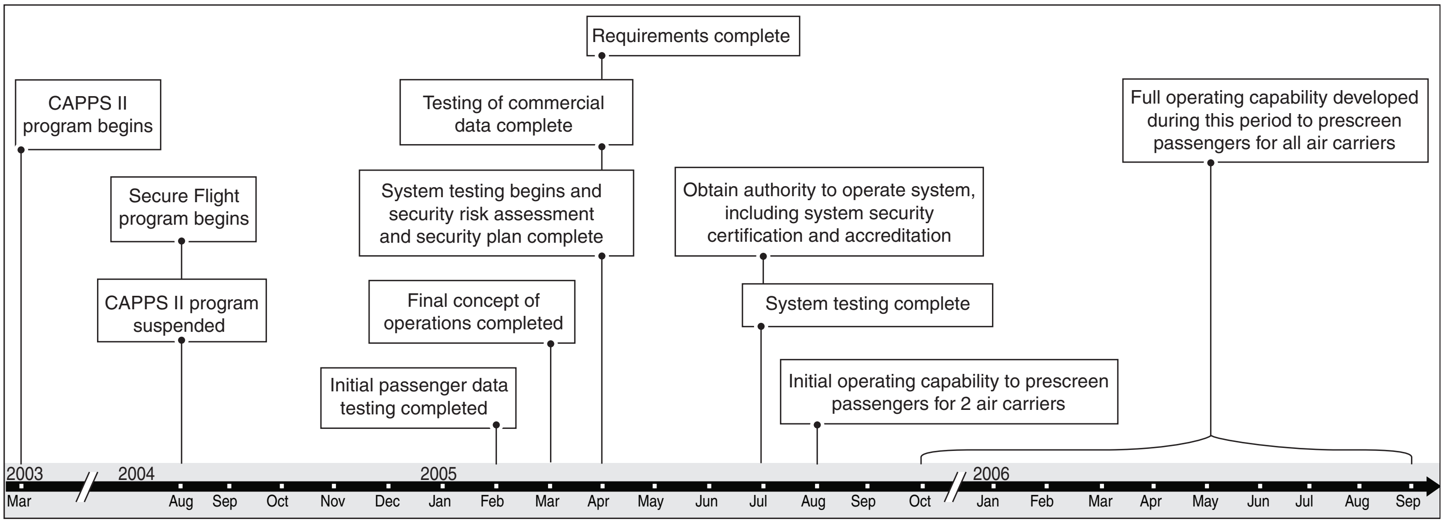
TSA Recently Developed a Comprehensive Schedule, but Key System Documentation and Development Activities Have Not Yet Been Completed

TSA is continuing the development of the centralized platform originally developed under CAPPS II—known as the Transportation Vetting Platform—and the Secure Flight application to conduct its prescreening activities. In continuing its development activities, TSA has developed a draft concept of operations, a draft system requirements document, and a project schedule to guide its efforts. However, these documents have not yet been finalized. These documents will need to be finalized in order to guide the system's development and to proceed with the final phases of testing. The concept of operations identifies to the eventual users of the system how the system will operate, while a detailed set of requirements agreed on by the government and the contractor helps ensure that Secure Flight is built with the desired functionality.

TSA completed a draft concept of operations in February 2005. This document provides a high-level perspective of how the system will operate and includes the roles and responsibilities of key staff and organizations. It also provides information necessary to begin finalizing other documents, such as system requirements. However, the concept of operations also identifies that many key decisions regarding Secure Flight operations have not yet been made. For example, the responsibilities between TSA's Office of Transportation Vetting and Credentialing, which is responsible for developing and implementing Secure Flight, and CBP, which TSA expects will provide the connectivity and data transport services to and from the airlines for Secure Flight, have not yet been determined. Further, TSA has not defined how the air carriers or airline reservations systems will interface with CBP. TSA acknowledges that not being able to obtain personally identifiable passenger data found in PNRs from the air carriers because of costs to the industry and lack of funding is an area of risk. TSA also recognized that it has to make these and other policy decisions before finalizing the concept of operations. However, TSA does not plan to finalize these documents until after completing the testing that is currently being conducted to determine Secure Flight's data needs and functions. According to TSA's schedule, the final concept of operations and the definition of requirements are expected to be completed in March 2005 and April 2005, respectively. The sooner these key documents are completed, the greater the chance TSA has of developing a system that meets its needs. With Secure Flight currently scheduled to prescreen its first passenger in August 2005, the lack of these key documents in final form increases the risk that TSA will develop a system that will not function as intended or meet TSA's needs.

In addition to the concept of operations and the system requirements documents, TSA uses a working milestone chart and a draft project schedule to guide its system development and testing activities. In February 2004, we reported that CAPPS II development was behind schedule and critical plans were incomplete. Specifically, TSA was behind schedule in testing and developing initial increments of the system, and had not yet established a complete plan to identify specific system functionality that would be delivered. We reported that TSA increased the risk of CAPPS II not providing expected functionality and of its deployment being delayed. TSA officials recognized that they had not fully developed CAPPS II with the thorough processes needed to properly develop a system. As a result, TSA officials stated that they are now attempting to build greater rigor into the Secure Flight development approach. During the transition from CAPPS II to Secure Flight, TSA modified its acquisition strategy and plan, obtained new contractors to develop and test Secure Flight, used another contractor to help develop key system documents and schedules, and hired more government personnel with knowledge and experience in project management. These steps have helped improve TSA's approach for the development of the Secure Flight system. For example, after announcing the start of Secure Flight in August 2004, TSA developed an initial working milestone chart in September 2004, and a more detailed draft integrated project schedule with milestones for developing, testing, and securing the system in November 2004. These documents provide information needed for program oversight officials, managers, and stakeholders to understand the projected and revised time frames for carrying out key activities. Figure 2 identifies TSA's projected key program milestones as of March 2005.

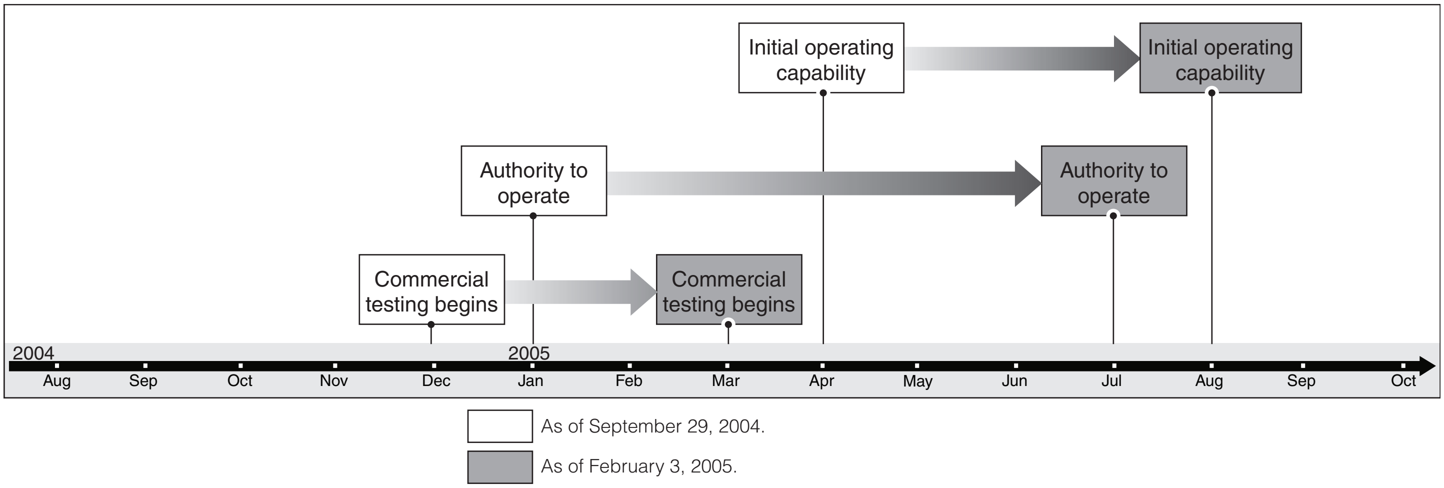
Figure 2: TSA Projected Key Milestones for the Development and Implementation of Secure Flight, as of March 2005


Requirements complete
CAPPS II program begins
Testing of commercial data complete
Full operating capability developed during this period to prescreen passengers for all air carriers
Secure Flight program begins
System testing begins and security risk assessment and security plan complete
Obtain authority to operate system, including system security certification and accreditation
CAPPS II program suspended
Final concept of operations completed
System testing complete
Initial passenger data testing completed
Initial operating capability to prescreen passengers for 2 air carriers
2003
2004
2005
2006
Mar
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep

Source: GAO analysis of TSA data.

Although TSA developed working milestones, TSA has revised its working milestone chart several times, as figure 3 illustrates. During the 5-month period between September 2004, when Secure Flight began, and February 2005, when the project plan was most recently revised, TSA delayed key milestones by up to 5 months. For example, TSA delayed the date Secure Flight is ready to begin prescreening passengers during initial operations, using two air carriers, from April 2005 to August 2005—a 4-month delay. According to TSA officials, they delayed initial operations and other key milestones since the Secure Flight program began because of a number of factors. For example, TSA officials stated they received more than 500 comments on the Secure Flight privacy notices, which caused delays in meeting key milestones. TSA officials identified that not meeting the Secure Flight schedule is a key risk that they plan to mitigate by assessing the program's progress against information technology program management standards and implementing tools to facilitate program execution, monitoring, and documentation.

Figure 3: Slippage in Key Secure Flight Milestones between September 2004 and February 2005

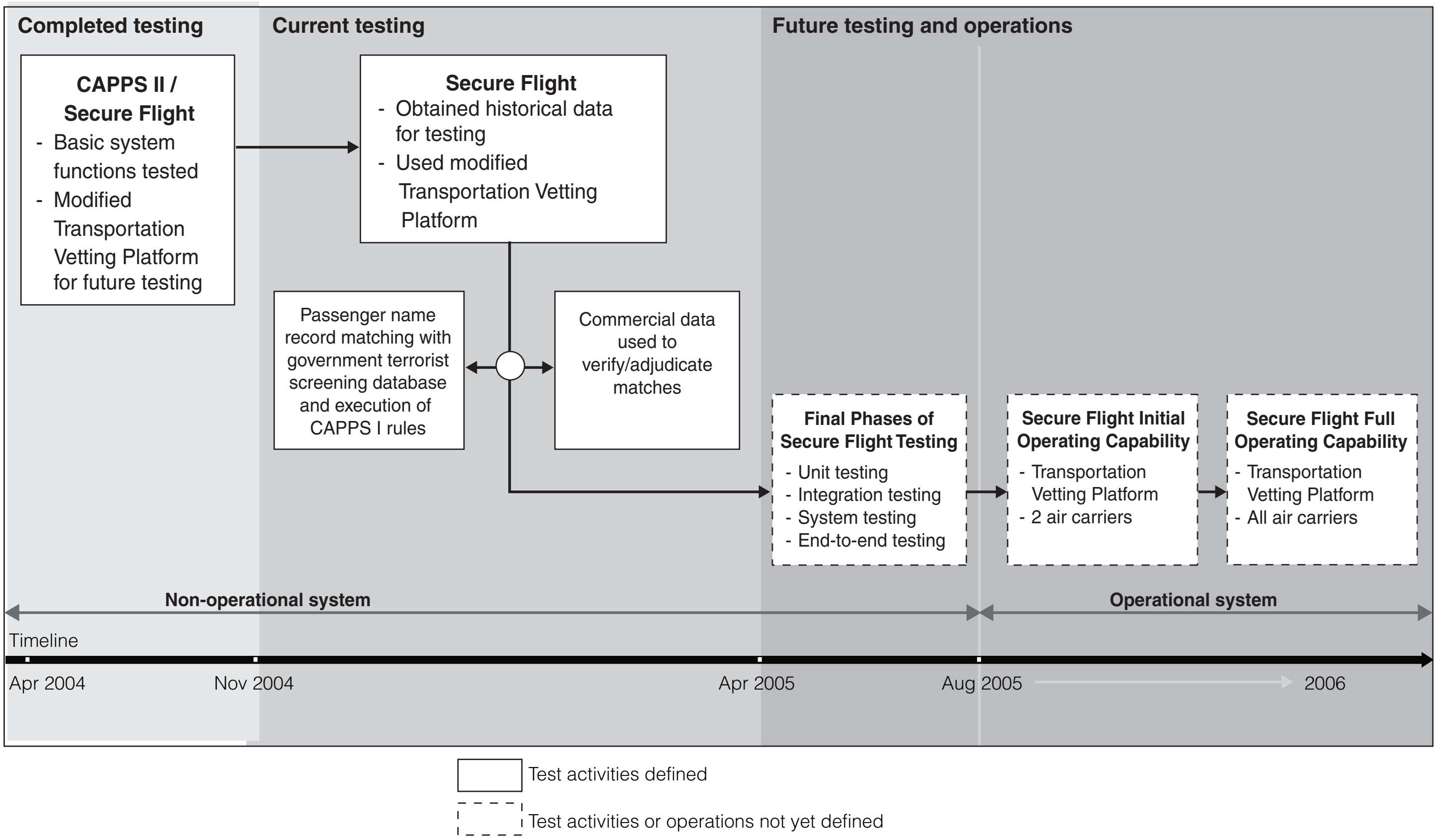


Source: GAO analysis of TSA data.

TSA Is Conducting Initial Testing, but Key System Testing Remains

TSA acknowledges the importance of testing the Secure Flight system to refine system requirements and help ensure desired functionality is achieved. TSA conducted some testing under the CAPPS II program that will benefit Secure Flight, and is currently completing additional testing to determine the information that will be needed in the passenger record to match PNR data against the TSC terrorist screening database and the CAPPS I rules, and plans to fully test the entire system before it becomes operational. TSA plans to conduct this system testing after key decisions are made about Secure Flight's functions, such as what passenger data will be used, which will be based in part on the results of current testing. Figure 4 summarizes TSA's completed, current, and future testing and operations for the Secure Flight system.

Figure 4: TSA's Completed, Current, and Future Planned Testing and Operations for Secure Flight


Completed testing
Current testing
Future testing and operations
CAPPS II / Secure Flight
- Basic system functions tested
- Modified Transportation Vetting Platform for future testing
Secure Flight
- Obtained historical data for testing
- Used modified Transportation Vetting Platform
Passenger name record matching with government terrorist screening database and execution of CAPPS I rules
Commercial data used to verify/adjudicate matches
Final Phases of Secure Flight Testing
- Unit testing
- Integration testing
- System testing
- End-to-end testing
Secure Flight Initial Operating Capability
- Transportation Vetting Platform
- 2 air carriers
Secure Flight Full Operating Capability
- Transportation Vetting Platform
- All air carriers
Non-operational system
Operational system
Timeline
Apr 2004
Nov 2004
Apr 2005
Aug 2005
2006
Test activities defined
Test activities or operations not yet defined

Source: GAO analysis of TSA data.

The testing phase of a system development project is used to help ensure that system functions meet their specified requirements. According to leading information technology organizations, to be effective, practices for testing software—such as that to be used in Secure Flight—should be planned and conducted in a structured and disciplined approach. Typically, this involves testing increasingly larger increments of a system until the complete system and all of its functionality are tested and accepted, and resolving critical problems before moving to the next phase of testing. It also involves stress testing and fully demonstrating the effectiveness and accuracy of the system. TSA's recently drafted Test and Evaluation Master Plan provides a high-level description of Secure Flight's overall test program and identifies TSA's plans to conduct the required tests. TSA also prepared detailed test plans for its current testing and will need to develop additional plans before beginning its future system tests, scheduled to begin in April 2005.

TSA Completed Initial Testing on CAPPS II System That Will Support Secure Flight Testing

Since April 2004, TSA has completed several tests on the CAPPS II and Secure Flight systems. In March and April 2004, TSA tested several components of the CAPPS II system including matching names against a basic watch list and applying the CAPPS I rules. To conduct these tests, TSA used simulated passenger data based on personal information volunteered by 32 government and contractor personnel who had originally worked on the CAPPS II program. When CAPPS II ended, several features had not yet been tested, including system effectiveness, security, privacy controls, system availability, backup and recovery, and system monitoring.

In November 2004, during the transition from CAPPS II to Secure Flight, TSA conducted several tests to verify that the system features brought forward from CAPPS II functioned as intended after modifications had been made for Secure Flight.[21] TSA used the same simulated passenger test data for these tests that it had used in April 2004. At the conclusion of these tests, according to TSA officials, they found that the watch list matching and CAPPS I rules application worked sufficiently well enough to move forward with the current testing phase of Secure Flight. However, our analysis shows that TSA tested only 28 percent of the system's requirements. According to TSA officials, they only tested the system requirements that were necessary to support initial performance testing. Officials further stated that they plan to test all Secure Flight requirements as part of the final phase of system testing beginning in April 2005.

TSA Currently Conducting Tests to Further Define Secure Flight Data Needs and Functionality

TSA is currently testing Secure Flight to determine (1) what data will be needed in the PNR for the system to most effectively match PNR data with data contained in the terrorist screening database and (2) whether commercial data (personal data, such as name, address, and phone number, maintained by private companies) can enhance the ability of Secure Flight to match PNR data with data contained in the terrorist screening database. To accomplish these tests—referred to as the PNR tests and commercial data concept tests, respectively—TSA obtained historical PNRs from domestic air carriers for passengers who flew flight

[21] As described earlier in this report, the scope of Secure Flight is more limited than CAPPS II. Therefore, several features of the CAPPS II system were deactivated, such as the identity authentication process and alert list capability.

segments beginning and completed during the month of June 2004.[22] TSA officials expect the results of these PNR and commercial data tests to allow them to make informed policy decisions regarding what passenger data will be required for Secure Flight operations. According to TSA officials, after these tests are completed, TSA plans to use the test results to help finalize the concept of operations and system requirements. For example, according to TSA officials, these tests could show that TSA may need air carriers to collect date of birth information, which is currently not collected by air carriers when taking reservations and could therefore delay system deployment, or TSA may need to pay for commercial data, which could increase system operating costs.

PNR testing: TSA recently completed testing that compares the various combinations of passenger-provided information contained in air carrier reservation systems,[23] known as PNR data, against data contained in the terrorist screening database, in order to identify individuals known or reasonably suspected to be engaged in terrorism. TSA developed test cases to help determine how effective Secure Flight is in identifying individuals who were incorrectly identified as being listed in the terrorist screening database (referred to as false positives), or individuals not identified as being on a terrorist watch list when in fact they should have been identified (referred to as false negatives). Preliminary test results of matching data in the terrorist screening database against various combinations of PNR data showed that watch list matching is possible; however, there are challenges in obtaining the data in a format that the system can use. Further, although TSA attempted to test the application of CAPPS I rules, the data provided by the air carriers were insufficient to test the CAPPS I rules as part of the Secure Flight program since not all of the data air carriers' require to run CAPPS I are contained in PNRs. We discuss these points in further detail later in this report.

[22] To obtain data for Secure Flight testing, TSA issued an order in November 2004 requiring domestic airlines to provide passenger records for the month of June 2004. Sixty-six air carriers, representing 99.8 percent of the total enplanements, provided more than 15 million PNRs.

[23] These reservation systems contain detailed information about an individual's travel on a particular flight, including information provided by the passenger when making a flight reservation. Such information can include (1) passenger name; (2) reservation date; (3) travel agency or agent; (4) travel itinerary information; (5) form of payment; (6) flight number; and (7) seating location.

Commercial data concept testing: TSA is currently conducting a concept test,[24] using commercial data to enhance or augment the June 2004 historical PNR data, to determine if the inclusion of additional information in the PNR can improve the matching of passenger-provided information against the terrorist screening database by reducing false positives and false negatives. The commercial data concept test is also intended to determine if the accuracy of passenger-provided data can be verified using commercial data. To determine the effectiveness of using commercial data, TSA developed initial measures for commercial data concept testing, such as the overall percentage of passenger-provided records from which identity can be verified using commercial data, and plans to refine the measures throughout the testing process.[25] TSA awarded a contract to conduct commercial data concept testing in February 2005, and expects to obtain the test results in April 2005. When these tests are completed, DHS and TSA plan to make policy decisions regarding the data elements that should be included in the PNR and whether commercial data will be used in support of the Secure Flight program. These critical decisions could lead to changes in system requirements.

TSA Plans to Conduct Stress Testing as Part of Final System Testing

Area of Congressional Interest: Stress Testing

Beginning in June 2005, TSA plans to conduct a series of tests consisting of increasingly larger increments of the system's functionality until the complete system is tested. These tests are designed to demonstrate the efficiency and accuracy of the entire system, including 100 percent of the requirements. This testing will include external interfaces for two-way data exchange between the air carriers and TSA, and also for obtaining data from the TSC. These tests will also include stress testing. Secure Flight has a stringent performance requirement to process 2.5 million transactions per day, with a peak load of 180,000 transactions within 10 minutes. During the PNR testing, TSA conducted limited stress tests of the system by running 1.8 million matching requests within 24 hours. TSA did not test the number of matches against its more stringent requirement of completing 180,000 matches within 10 minutes. Further, these results are based on testing that did not involve the entire system, including

[24] The purpose of the concept test is limited to identifying the utility of using commercial data in improving the effectiveness of comparing passenger information against the terrorist watch list in a test environment.

[25] In February 2005, we issued a report assessing TSA's measures for commercial data testing. GAO, *Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program*, GAO-05-324 (Washington, D.C.: Feb. 23, 2005). We also have an ongoing follow-up review examining the Secure Flight commercial data testing process and will report to Congress on our findings.

connectivity to air carriers and the possible application of CAPPS I rules. Although TSA conducted the limited stress testing, it is planning to conduct system stress tests that are designed to help ensure that Secure Flight can operate efficiently, accurately, and during peak load, and will use test results to determine system readiness to operate live with two carriers by August 2005. Table 4 identifies TSA's planned milestones for its final phases of system testing.

Table 4: TSA's Schedule for Final Phases of Secure Flight Testing

Testing activity	Purpose	Begin	End
Unit testing	To verify that the smallest defined module of the system works as intended before integrating with other modules	April 20, 2005	May 31, 2005
Integration testing	To verify that units of the system, when combined, work together as intended	June 1, 2005	June 9, 2005
System testing	To verify that the complete system (all the units combined) satisfies specific requirements such as functionality, performance, and security	June 9, 2005	June 23, 2005
End-to-end testing	To verify that the entire system, including any external systems with which it interfaces, functions as intended in an operational environment	June 23, 2005	July 15, 2005

Source: GAO analysis of TSA data.

Although TSA has developed this testing schedule and has described its overall strategy for conducting these tests, it has not yet developed the detailed test plans needed for unit, integration, system, and end-to-end testing, which are scheduled to begin in April 2005. TSA officials stated that they have identified a time frame during end-to-end testing when they plan to conduct performance and complete system stress testing. However, officials stated that the specific test plans cannot be finalized until TSA makes key decisions regarding the final operational and functional requirements for Secure Flight. Until TSA develops detailed and complete test plans and fully executes these plans, it is unknown how well Secure Flight will perform and whether it will be ready to be operational with two air carriers in August 2005.

TSA Is Taking Steps to Improve the Ability of Secure Flight to Identify Passengers Who Should Undergo Additional Security Scrutiny, but System Effectiveness Has Not Been Determined

Area of Congressional Interest: Accuracy of Databases and Effectiveness of Secure Flight

TSA has begun, or has plans to initiate, a number of actions designed to improve the ability of Secure Flight to identify passengers who should undergo additional security scrutiny, relative to the prescreening currently conducted by the air carriers. These actions are in response to the 9/11 Commission's recommendation that the government improve passenger prescreening by taking over, from the air carriers, responsibility for prescreening passengers using an expanded set of terrorist watch lists currently not available to air carriers. TSA efforts to strengthen passenger prescreening include conducting initial testing, prior to the further development and implementation of Secure Flight, to identify the most effective combination of data elements in PNR and the terrorist screening database to be matched. TSA also plans to use intelligence analysts to help resolve discrepancies in the matching of PNR data to data contained in the terrorist screening database, and recently modified the CAPPS I rules to facilitate more targeted screening of individuals.

Although TSA is taking these actions, the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny has not yet been determined, and can be affected by data quality and other factors. Specifically, TSA officials reported that recently completed testing identified an improvement in Secure Flight's ability to match PNR data to data contained in the terrorist screening database over watch list matching conducted by the air carriers. However, key issues regarding how these data will be obtained and transmitted have not yet been resolved. Further, as is the case with the current airline-operated process of matching passenger names against no-fly and selectee lists—which are extracted from the terrorist screening database and provided by TSA—the ability of Secure Flight to make accurate matches between PNR data and data contained in the terrorist screening database is dependent on the type and quality of data contained in the database as well as in PNRs. While TSC and TSA have taken, or plan to take, a number of actions to improve the quality of the data in the terrorist screening database, the accuracy of the database has not been determined. The effectiveness of data matches will also be dependent on the accuracy of commercial data used to augment the matching, should TSA decide to use commercial data for Secure Flight. However, the accuracy of commercial data is undetermined because there are no industry standards for processes or requirements to ensure accuracy. Further, although TSA recently modified CAPPS I rules to result in more targeted screening, TSA has been unable to determine the impact of these changes on the screening process, and may not be able to obtain all of the information needed to apply the rules from PNR data. Another factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's ability to identify passengers who assume the identity of another individual, known as identity theft.

Initial Secure Flight Test Results Show Improvements over Current Passenger Prescreening, but Key Issues Regarding How Data Will Be Obtained and Transmitted Have Not Yet Been Resolved

TSA recently completed testing intended to help identify those data elements in both PNR data and the terrorist screening database that will be needed to make the most accurate matches, and to identify error rates that occur with the various combinations of data elements being matched. Specifically, TSA matched different combinations of data elements from both PNR data and data contained in the terrorist screening database, such as last name only, full name only, or full name and date of birth. TSA is in the process of analyzing the results of these tests to determine which data elements would be most effective for successful matching once Secure Flight becomes operational. TSA also identified estimated error rates in matching PNR data with data contained in the terrorist screening database under the various combinations of data matched. In the context of Secure Flight, errors occur if an individual is incorrectly identified as being on a terrorist watch list (referred to as a false positive) or if an individual is not identified as being on a terrorist watch list when in fact he or she should have been identified (referred to as a false negative). According to TSA, these test results will be used to help determine whether additional or different combinations of data are needed to help reduce error rates. TSA will also use this data to determine whether identified error rates are acceptable and whether additional work will be required to reduce these rates.

Although initial PNR testing was only recently completed, and test results have not been fully documented and analyzed, TSA officials stated that these results show that Secure Flight will be more effective in matching PNR data with data contained in the terrorist screening database than matches currently conducted by the air carriers. Specifically, TSA officials believe that the results showed that Secure Flight will be capable of detecting names that are exact matches as well as minor variations in names with information in the terrorist screening database. TSA officials further stated that test results indicate that adding date of birth to PNR data may further reduce the number of false positives. However, according to TSA officials, the affect of adding date of birth on false negative rates was less clear. Because this testing has only recently been completed and test results have not been fully compiled and analyzed by TSA, we were unable to independently assess these results. Specifically, we did not independently assess whether the results showed an improved capability over the current air carrier process, or the basis from which this measurement was made. TSA officials stated that they would continue to review the recently completed test results before making decisions regarding the data to be used in Secure Flight.

Although TSA believes, based on initial test results, that Secure Flight can effectively match PNR data with data contained in the terrorist screening database, key issues regarding how these data will be obtained and transmitted have not yet been resolved. Specifically, TSA officials have not yet determined what data elements they will require to be collected in PNR data and what data elements will be needed from the terrorist screening database to support Secure Flight operations. Based on test results, TSA officials stated that requiring airlines to collect full name and date of birth in PNR data will ultimately increase the effectiveness of data matches. However, air carriers are not currently required to collect full name and date of birth information in PNR data. Requiring air carriers to collect this information could require significant changes to their reservation systems and could take time to implement. TSA plans to identify required data elements that must be collected in PNRs in April 2005. TSA also plans to identify data requirements from the terrorist screening database, through a memorandum of understanding with the TSC, expected to be finalized in May 2005.

Further, although TSA officials stated that CBP will provide connectivity between the air carriers and Secure Flight, TSA has not yet developed a plan identifying how connections will be made between air carrier reservation systems and TSA to support Secure Flight prescreening. Currently, international air carriers have a one-way connection through the existing infrastructure that supports the Advanced Passenger Information System, which allows them to send data to CBP, but does not allow air carriers to receive data.[26] According to TSA officials, they are working with CBP to resolve how air carriers could both send and receive data, as air carriers would have to receive information from Secure Flight, after data matches have occurred, to identify whether passengers will require additional security attention. TSA will also need to resolve how data will be transmitted between smaller airports and carriers that fly only domestically and therefore do not currently have an established connection through CBP. TSA officials stated that CBP's current communications infrastructure would need minor enhancements in order

[26] The Advanced Passenger Information System, maintained by CBP, is an automated system used to prescreen passengers and crew members prior to their arrival in or departure from the United States.

to support Secure Flight's initial operating capability with two air carriers. However, officials from CBP stated that it is unclear whether the current communications infrastructure used by the Advanced Passenger Information System can handle the high volume of data that would be required to be transmitted to support Secure Flight once it is fully operational. According to TSA officials, they plan to resolve these and additional issues with CBP during Secure Flight's initial operations with two air carriers.

TSA identified the ability of the airline industry to provide TSA with the PNR data needed to support Secure Flight operations as a key program risk because of potential costs to the industry of changes to their reservation and other systems that may be required. TSA also noted that establishing a connection between the air carriers and TSA to transmit data is a risk, and that potential requirements for additional PNR data could result in boarding delays. TSA plans to mitigate these risks by supporting the development of a funding strategy to reduce and defray expenses to air carriers and other transportation industries. However, TSA has not described how it plans to do this. TSA also plans to coordinate the development of operating policies and procedures with officials from CBP, TSC, select airline industry officials, and industry technical working groups.

Efforts Are Being Taken to Improve the Quality of Data That Will Support Secure Flight Operations, but the Accuracy of These Data Has Not Been Determined

In order to identify individuals known or suspected to be engaged in terrorism, Secure Flight plans to compare PNR data with information contained in the terrorist screening database, a database that is government-owned and controlled by the TSC. The TSC is responsible for maintaining the accuracy of the information contained in the terrorist screening database.[27] Although a senior TSC official stated that the TSC considers the data in the terrorist screening database to be accurate, the official stated that the underlying accuracy of the data has not been fully determined, and that the TSC does not know with certainty whether errors in the database may exist, such as incorrect name or date of birth. According to TSC officials, the underlying accuracy of the data is dependent upon a number of factors outside the control of the TSC, such

[27] According to TSC officials, the TSC is dedicated to maintaining "the most thorough, accurate, and current information possible" about individuals in its database in accordance with the *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism*, dated September 16, 2003.

as the process used by nominating agencies to assess the information and the reliability of sources.

While the complete accuracy of data contained in this database can never be certain—given the varying quality of intelligence information gathered, and changes in this information over time—TSC has established processes to help ensure the quality of these data. For example, in order to add an entry to the database, an agency must go through a nomination process in which representatives from the nominating agency review available information and make a determination whether the person should be included in the database.[28] Another quality control mechanism to improve the accuracy of data, according to the TSC official, involves the process of removing records from the database. The TSC has the sole authority to remove records from the database. Each time a record within the database is searched, TSC is to reexamine the record to ensure that the information can be substantiated. If the information cannot be substantiated, TSC can remove the record from the database. According to the TSC official, approximately 4,800 records have been removed from the database as of December 16, 2004.[29]

In order to match PNR data to information contained in the terrorist screening database, TSC plans to provide TSA with daily copies of a subset of the database for use in Secure Flight. All individuals listed in the data subset are to be designated as either selectees (will be required to undergo secondary screening before being permitted to board an aircraft) or as no-flys (will be denied boarding unless they are cleared by law enforcement personnel). TSA officials stated they would not receive the entire terrorist screening database because certain portions of the database do not contain basic elements required for Secure Flight matching (e.g., full name). TSA officials further stated that they do not plan to assess the accuracy of the data provided by TSC prior to matching PNR data against data contained in the database because assessing the accuracy of the data is the responsibility of TSC and the nominating agencies. That is, officials stated that they will not attempt to determine whether individuals listed in the database are inappropriately identified as being associated with

[28] Domestic terrorist nominations come through the Federal Bureau of Investigations. International terrorist nominations come through the National Counter Terrorism Center, which was formerly the Terrorist Threat Integration Center.

[29] GAO has an ongoing review examining the reliability and accuracy of the TSC terrorist screening database.

terrorism, and will not attempt to determine if specific data contained in the database are accurate, such as name spelling, date of birth, or passport number. However, TSA officials stated that as a nominating agency for the terrorist screening database, TSA works with TSC to increase the quality of the entries nominated by TSA. TSA officials also noted that accuracy of the data provided by TSC is also not assessed under the current prescreening program operated by the air carriers.

TSA is also considering using commercial data to validate PNR data by comparing these records against information contained in commercial databases, or to augment incomplete passenger records, as PNR data are matched against data in the terrorist screening database.[30] However, the accuracy of commercial data is uncertain, which could limit the effectiveness of these data in helping to make accurate matches of PNR data to data contained in the terrorist screening database for Secure Flight. As we reported in February 2004, commercial data providers use varied measures and criteria to assess accuracy, and there are no industry standards for processes or requirements to ensure accuracy. We also reported that even databases determined to have an acceptable level of accuracy will still contain errors.[31] As part of commercial data testing that TSA began in February 2005, TSA plans to review methods for assessing the types and quality of data available from commercial sources, as well as the relative accuracy of commercial data products.[32] However, TSA has not yet decided how the accuracy of these data will be determined, or what an acceptable level of accuracy would be in terms of Secure Flight. If the data in commercial databases are determined to have an unacceptable level of accuracy to support Secure Flight operations, the usefulness of commercial data in augmenting data contained in PNRs may be limited.

Although TSA does not plan to assess the accuracy of data contained in the terrorist screening database, and recognizes that the accuracy of commercial data is uncertain, TSA expects to improve the accuracy of data used to support Secure Flight operations, over time, through the development of a redress process to provide passengers, who believe they were inappropriately delayed from boarding their scheduled flights

[30] Commercial data are maintained by private companies and can include personally identifiable information that either identifies an individual or is directly attributed to an individual, such as name, address, and phone number.

[31] GAO-04-385.

[32] TSA expects commercial data testing to be completed by April 2005.

because of Secure Flight, a means by which to appeal these decisions. Specifically, TSA expects that the redress process will help identify inaccurate data contained in the terrorist screening database or commercial databases, should TSA decide to use them, which in turn could potentially be corrected. Under the proposed Secure Flight redress process, TSA officials stated that TSC has agreed in concept to investigate—if passengers seek redress because they believe they were inappropriately targeted for additional security scrutiny by Secure Flight—the reason a person was listed in the database, including consulting with the originating agency and removing a person from the database if appropriate. However, TSA has not determined how this process is likely to work in practice, or worked out the agreements needed with TSC on how the data will be corrected. TSA's ability to correct data in commercial databases is also questionable. The Secure Flight draft redress policy indicates that TSA will be responsible for identifying errors in commercial databases, should TSA decide to use them for Secure Flight, and will work with commercial data aggregators (who maintain the commercial databases) to correct errors, should those errors result in passengers being incorrectly selected for additional screening. However, it could be difficult to correct errors found in commercial databases because data aggregators purchase their data from other sources and may not be obligated to correct the data. Moreover, data aggregators may not be permitted to share the source of their data. In order to be most effective, errors would need to be corrected at the source. Without information on how these processes will be implemented, it is too early to determine whether they will be effective in improving the quality of data matches. TSA plans for a Secure Flight redress process are discussed in greater detail later in this report.

TSA plans to use intelligence analysts during the actual matching of PNR data to data contained in the terrorist screening database to increase the accuracy of data matches. Specifically, TSA plans to have intelligence analysts staffed within TSA to identify false positives—passengers inappropriately matched against data contained in the terrorist screening database—as PNR data are matched against data in the terrorist screening database, and resolve mistakes to the extent possible before inconveniencing passengers. One of the goals of Secure Flight testing is to determine the number of TSA intelligence analysts that will be required to clear misidentified passengers. However, TSA has not yet determined how the TSA intelligence analysts will consult with TSC to obtain the information necessary to increase the accuracy of data matches. Accordingly, the effectiveness of using intelligence analysts to clear misidentified passengers during Secure Flight operations is unclear.[33]

Changes to CAPPS I Rules May Result in More Targeted Security Screening, but Potential Benefits to Secure Flight Are Not Yet Known

Area of Congressional Interest: Modifications with Respect to Intrastate Travel to Accommodate States with Unique Air Transportation Needs

TSA recently modified the passenger screening criteria currently used by the CAPPS I system, known as the CAPPS I rules, to facilitate more targeted screening of individuals and to reduce the number of passengers selected for additional security scrutiny— termed selectees.[34] As described earlier, passenger prescreening will encompass the matching of PNR data to data contained in the terrorist screening database and the application of CAPPS I rules. TSA has attempted to conduct testing to determine the impact of CAPPS I rules changes on estimated selectee rates for Secure Flight. However, since air carriers' PNRs do not contain all of the data required to run CAPPS I, the data provided by the air carriers were insufficient to enable TSA to determine the impact of these changes on selectee rates. Further, TSA has not yet determined whether it will assume the CAPPS I rules application as part of the Secure Flight program or whether air carriers will continue to apply CAPPS I rules. Should TSA decide to incorporate the application of CAPPS I rules into Secure Flight, it will need to resolve how the system will obtain the necessary data from the air carriers, since some of the data needed for the operation of CAPPS I are not currently contained in PNRs.

Currently, air carriers prescreen passengers using CAPPS I, which identifies selectees by comparing passenger information found in the PNR and other air carrier passenger data systems with a set of characteristics, known as CAPPS I rules. CAPPS I is not specifically intended to identify individuals known or suspected to be associated with terrorism. However, TSA considers CAPPS I to be an effective risk management tool by helping to identify the relatively small number of passengers whose PNR data correlates closely with the behaviors of terrorists.

TSA officials stated that recent changes in the airline industry have produced disproportionably high selectee rates for certain air carriers as a result of certain CAPPS I rules. To address this issue, TSA officials stated that the agency's Aviation Operations group conducted an analysis of the

[33] According to TSA, it currently uses intelligence analysts to perform similar functions for a variety of other programs.

[34] CAPPS I rules are Sensitive Security Information.

CAPPS I rules. As a result of this effort, TSA officials reported that they have changed certain CAPPS I rules, which they believe will reduce overall selectee rates. Although changes to these CAPPS I rules were not specifically intended to respond to concerns of any particular state or air carrier with regard to selectee rates, TSA officials stated that the changes should reduce the overall CAPPS I selectee rate thereby addressing some of the concerns of states with unique air transportation needs and high selectee rates.

Although TSA does not have estimates for the selectee rates for any particular state, TSA has estimated the variability of selectee rates for different types of air carriers. While TSA estimates the overall selectee rate for air carriers is 15 percent, more detailed TSA estimates of selectee rates, such as rates for specific air carriers, and potential affects of CAPPS I rules changes are Sensitive Security Information and have been removed from this report. Accordingly, we are issuing a separate letter summarizing this information in more detail.[35]

TSA officials expected that Secure Flight testing would allow TSA to more accurately identify the effect of CAPPS I rule changes on the selectee rate, to determine whether these changes will result in more targeted and effective security screening and reduce selectee rates. Specifically, TSA had planned to identify actual selectee rates by comparing the June 2004 historical PNR data it obtained for testing against the CAPPS I rules that were in effect during that month. Using that selectee rate as a baseline, TSA planned to determine the selectee rate using the modified CAPPS I rules to measure any changes. However, TSA could not determine the effect of the CAPPS I rule changes on selectee rates because PNR data that TSA obtained from the air carriers for testing did not contain all of the information needed to run CAPPS I rules, since some of the information needed was contained in other air carrier databases.[36] Without these data, the effect of the CAPPS I rule changes in conducting more targeted screening cannot be determined. Further, TSA has not yet determined whether it will assume the CAPPS I rules application as part of the Secure Flight program or whether air carriers will continue to apply CAPPS I

[35] GAO-05-445SU.

[36] According to TSA, one air carrier provided sufficient data for TSA to test the application of CAPPS I rules. TSA reported that the results of that test indicated a potential reduction in the number of selectees. However, because this testing has only recently been completed, we were unable to independently assess the results.

rules. Should TSA decide to incorporate the application of CAPPS I rules into Secure Flight, it will need to resolve how the system will obtain the necessary data from the air carriers, since not all of the data needed are currently contained in PNRs.

False Identifying Information and Identity Theft Could Affect the Security Benefits of Secure Flight

Another factor that could affect how well Secure Flight identifies known or suspected terrorists is the system's ability to identify passengers who falsify their identifying information or who commit identity theft. Falsifying identifying information involves passengers attempting to hide their true identities by submitting fictitious identifying information, such as false addresses, when purchasing tickets. Identity theft would involve a passenger "stealing" another person's identifying information, such as name and date of birth, and then using that identifying information to create fraudulent documents associated with the identity (such as a driver's license containing the stolen identifiers with the thief's picture).[37] As our previous work has shown, identity theft is growing in this country.[38]

TSA officials recognize that checking passenger information contained in PNRs against information contained in the terrorist screening database, which will be the basis of Secure Flight operations, will not identify those using a stolen identity. TSA officials further stated that Secure Flight is not intended to address identity theft, but rather is designed to take over the responsibility, from air carriers, of matching passenger data against terrorist watch lists. The current prescreening process of matching passenger names against no-fly and selectee lists also does not address identity theft.

Although TSA acknowledged that Secure Flight cannot fully address the creation of false identifying information or identity theft, officials stated that the use of commercial data may help identify situations in which a passenger submits fictitious information such as a false address. TSA officials are examining whether the use of commercial data could detect these instances because the data being provided by the passenger would either not be validated or would be inconsistent with the information maintained by the commercial data provider. However, whether the use of commercial data will assist Secure Flight in identifying fictitious

[37] This is sometimes referred to as identity fraud.

[38] GAO, *Identity Theft: Prevalence and Cost Appear to Be Growing*, GAO-02-363 (Washington, D.C.: Mar.1, 2002).

information cannot be determined until commercial data testing is complete. Further, using commercial data would likely not be able to detect instances of identity theft involving stolen identifying information of an individual. TSA is conducting tests, using commercial data, to determine the extent to which commercial data can address fictitious identities as well as mitigate false positives and false negatives in the matching of passenger PNR data to data contained in the terrorist screening database. Based on the results of these tests, TSA plans to decide whether to incorporate the use of commercial data as part of Secure Flight.

TSA officials further stated that passenger information will continue to be compared against CAPPS I rules, whether by the air carriers or by TSA. While CAPPS I rules are not designed to address the creation of false identifying information or identity theft, TSA believes the application of CAPPS I rules—which are not dependent upon passenger identity—can provide an additional security layer. In addition, the CAPPS I process randomly identifies some airline passengers as selectees—passengers who were not initially selected based on CAPPS I rules—to ensure that no passenger is guaranteed selectee-free status. TSA officials further stated that Secure Flight is just one layer in a series of systems designed to strengthen aviation security, and that passengers who were able to thwart Secure Flight by committing identity theft would still need to go through normal checkpoint screening and other standard security procedures.

TSA officials recognized that Secure Flight would best address identity theft by implementing some type of biometric technology. As noted in our previous work, the seven leading biometric technologies are facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature recognition, and speaker recognition.[39] According to TSA officials, incorporating biometrics into the Secure Flight program is not currently envisioned. However, TSA plans to expand the Registered Traveler program, which uses biometrics to verify passenger identity. Although TSA has not determined how Secure Flight and Registered Traveler will be integrated, if at all, TSA officials stated that expanding the Registered Traveler program could help alleviate the problem of identity theft with respect to Secure Flight since passengers must verify their identity with a biometric captured during program enrollment and

[39] GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

assessed every time they fly. The Registered Traveler program is currently operating in the pilot phase at five airports. According to TSA officials, approximately 10,000 people are participating in the Registered Traveler pilot program.

DHS and TSA Have Taken Actions to Strengthen Their Oversight and Management of Secure Flight, but Key Issues Will Need to Be Resolved as the Program Is Further Developed

DHS and TSA have taken a number of actions designed to strengthen their oversight and management of Secure Flight. These efforts include providing oversight through a number of boards and working groups designed to manage the program's development and implementation. TSA also strengthened its oversight of Secure Flight contractors through various methods, including increasing the number of TSA staff with contract oversight responsibilities and recently finalizing an acquisition plan for Secure Flight and the Transportation Vetting Platform. TSA officials further engaged in outreach to key external stakeholders, to include air carriers, who they identified as integral to the successful implementation and operations of the Secure Flight program. These efforts should help DHS and TSA in managing their development and implementation efforts and help ensure, as the development of Secure Flight progresses, that key risks are identified and managed.

Although DHS and TSA have taken action to strengthen their oversight and management of Secure Flight, key issues will need to be resolved as program requirements are finalized, system testing is completed, and Secure Flight becomes operational. For example, TSA has not yet developed oversight policies governing the use and operation of the system, or finalized performance measures to measure program results. Further, although TSA is working with key external stakeholders who will be integral to Secure Flight operations, officials from some of these organizations expressed concerns to us regarding the uncertainty of Secure Flight system and data requirements, and the impact these requirements may have on the airline industry. TSA also has not finalized a security risk assessment and security plan, nor has it developed life-cycle cost estimates and only recently finalized an expenditure plan. TSA has recognized the importance of these plans and estimates to the successful implementation of Secure Flight, and because of uncertainties regarding program requirements—such as the possible use of commercial data—TSA identified system security and life-cycle costs as key program risks. Because plans addressing program operations, security, and costs are not fully developed, and key issues affecting the program—such as data requirements and connectivity to air carriers—have not been resolved, it will be important for established and planned oversight and management bodies to ensure that key program risks are appropriately managed.

DHS Oversight Board and External Advisory Committee Are in Place to Oversee the Development and Implementation of Secure Flight

Area of Congressional Interest: Internal Oversight Board for Secure Flight

Oversight mechanisms operate through a number of boards and working groups within DHS and TSA to oversee the development and implementation of Secure Flight. Each of these groups has a distinct role, ranging from overseeing the program at the executive level to providing TSA with comments on actions and processes related to information technology and privacy protection issues. These varying levels of oversight can help provide assurance that Secure Flight development and implementation issues are considered throughout the program's development. However, as development continues and Secure Flight becomes operational, it will be important that a consistent and continuing level of oversight be provided to monitor the program's progress and manage risks as system requirements and operations are refined, and that issues identified by these oversight bodies are fully addressed, given the state of Secure Flight's development.

Acquisition Oversight Is Provided by DHS

DHS established an Investment Review Board to provide executive-level review of department and agency acquisition activities. The Investment Review Board consists of senior DHS executives and is chaired by the Deputy Secretary. The board is tasked with reviewing all capital assets with contracts exceeding $50 million, and all information technology programs with expected life-cycle costs in excess of $200 million.[40] The board's purpose in reviewing programs meeting these thresholds during key phases of program development is to help ensure that programs meet mission needs at expected levels of cost and risk.[41]

To date, the DHS Investment Review Board has reviewed the Transportation Vetting Platform[42] —from which Secure Flight will operate—and Secure Flight one time, on January 27, 2005. As a result of this review, the board withheld approval for the Transportation Vetting Platform and Secure Flight to proceed into the production and deployment phase until three issues were addressed. These issues included requiring that a formal acquisition plan be developed and approved for the platform by February 22, 2005; developing a plan for integrating and coordinating the platform with other DHS "people screening" programs; and

[40] DHS is currently revising their policy governing the thresholds for review by the DHS Investment Review Board.

[41] TSA programs are reviewed by the TSA Investment Review Board prior to review by the DHS Investment Review Board.

[42] The Transportation Vetting Platform is intended to provide screening services for a number of DHS programs, such as Secure Flight and Crew Vetting.

resubmitting a revised acquisition program baseline (cost, schedule, and performance parameters). In response to these requirements, TSA officials stated that they have revised the acquisition plan and the acquisition program baseline, and participated in a cross-agency working group to develop a plan for coordinating “people screening” programs within DHS. In doing so, TSA officials stated they have met all the requirements of the DHS Investment Review Board. However, TSA has not yet received approval from the DHS Investment Review Board to proceed. The DHS Investment Review Board further noted that additional concerns remained regarding system privacy protections and data security, and because of the platform’s and Secure Flight’s aggressive schedule, the risks of not meeting cost, schedule, and performance goals remained. The DHS Investment Review Board plans to meet again to review the Transportation Vetting Platform and Secure Flight when commercial data testing is complete, or no later than the spring of 2005. However, as we previously reported, DHS officials stated that the Investment Review Board was having difficulty reviewing all of the critical departmental programs in a timely manner.[43] Considering the risks identified by the Investment Review Board, it will be important that it continue to review the development and implementation of the Transportation Vetting Platform and Secure Flight as these programs move forward.

External Advisory Committee Designed to Provide Advice and Assistance for Secure Flight

In addition to the DHS Investment Review Board, the Aviation Security Advisory Committee established a Secure Flight working group to provide TSA with advice and assistance related to the development and implementation of the program. The advisory committee, now within DHS, is a standing committee created in 1989 in the wake of the explosion of Pan Am Flight 103 over Lockerbie, Scotland. The advisory committee is composed of federal and private sector organizations and was created to provide advice on a variety of aviation security issues. The Secure Flight Working Group, within the advisory committee, was formed in September 2004 to provide the committee with comments on actions, procedures, and processes related to the initial testing phase of Secure Flight. The working group is chaired by the TSA Privacy Officer and includes representatives from privacy advocacy groups, academia, and information technology firms. The primary focus of the working group is on privacy and information technology issues. Among other things, the working group is designed to review the initial testing phase of Secure Flight to provide advice on whether information used by the program is adequately

[43] GAO-04-385.

protected and secure, as well as review Secure Flight redress and appeals procedures regarding their timeliness, sufficiency, and ease of use. According to TSA officials, the working group has met four times. Following the completion of initial Secure Flight testing, scheduled for April 2005, the working group plans to incorporate its findings into a report to be presented to the advisory committee for its review and approval and to transmit the report to TSA. A TSA official stated the agency is considering continuing the working group beyond the Secure Flight initial testing phase.

TSA Has Taken Steps to Strengthen Contractor Oversight and Acquisition Planning, but Risks Remain

Recognizing problems in providing contractor oversight during the development of CAPPS II, TSA has reported strengthening its oversight of Secure Flight contractors and acquisition planning. According to TSA officials, the successful development and implementation of Secure Flight is heavily dependent on contractor performance and TSA's acquisition strategy. TSA's strategy involves reliance on contractors to provide many of the developmental and testing services for Secure Flight, while TSA's role is primarily to manage the program by providing program support, oversight of contractor activities, and technical expertise. TSA currently has two contractors dedicated to Secure Flight testing—one for testing PNR data matching against the TSC terrorist screening database, and one for testing the use of commercial data. TSA also oversees other contractors dedicated to the development and testing of the Transportation Vetting Platform.

According to TSA officials, governmental oversight of the CAPPS II program was limited. Specifically, TSA acknowledged that the program office responsible for developing CAPPS II was understaffed in terms of government employees and relied heavily on contractors to work under limited TSA oversight. As a result, TSA officials stated they did not always have assurance that the contractor was meeting its expected goals. Our previous work assessing TSA's overall acquisition management capability found similar problems across the agency. In May 2004, we reported that TSA had not developed an acquisition capability that facilitated the successful management and execution of acquisition activities.[44] We also found that TSA's acquisition policies and procedures had not been effectively communicated across the agency. Since our review, TSA has

[44] GAO, *Transportation Security Administration: High-Level Attention Needed to Strengthen Acquisition Function*, GAO-04-544 (Washington, D.C.: May 28, 2004).

taken steps intended to strengthen its contract management and oversight efforts. TSA officials stated that their contract oversight capability has been maturing in recent months, and that the agency now uses improved tracking mechanisms to monitor contractor schedule and cost information. TSA officials further stated that since program managers lacked adequate staff to gather and evaluate information needed for effective oversight, the agency uses several support contractors to assist with these tasks.

In addition to the agency's overall efforts to improve contract management, TSA officials also reported taking steps to strengthen contractor oversight for Secure Flight. For example, the Secure Flight program is using one of TSA's support contractors to help track the progress of the contractors developing Secure Flight in the areas of cost, schedule, and performance. Program officials stated they meet with the support contractor on a weekly basis and obtain frequent reports on the Secure Flight contractors' performance. TSA officials also stated they have increased the number of TSA staff with oversight responsibilities for Secure Flight contracts. Since TSA is relying on a support contractor to provide direct oversight over other contractors developing and testing Secure Flight, it will be important that TSA maintain strong oversight.

TSA also recently developed an acquisition plan that presents the acquisition strategy for the Secure Flight and the Transportation Vetting Platform. Acquisition plans, which set forth the overall strategy for managing a system's acquisition, are intended to help ensure that the government meets its needs in a timely manner and at a reasonable cost. Organizations within TSA are expected to use acquisition planning as an opportunity to evaluate and review the entire acquisition process so that sound judgments and decision making can help facilitate program success. Although best practices show that acquisition planning should begin as soon as the agency need is identified, with reviews and updates as needed, TSA has only recently finalized the acquisition plan for Secure Flight and the Transportation Vetting Platform. TSA officials cited the organizational changes within the Secure Flight program office as slowing their progress in developing the plan.

Although TSA has taken steps to strengthen contract oversight and acquisition planning, TSA has identified contract management as a key risk facing the development and implementation of Secure Flight. To mitigate this risk, TSA plans to develop communication mechanisms among DHS acquisitions officials, Secure Flight contractors, and Secure Flight program management officials. However, TSA has not yet defined what these mechanisms are or how they are intended to work. TSA also intends to use its acquisition plan to identify strategies for improving contract management. Since the successful development and implementation of Secure Flight is heavily dependent on contractor performance and TSA's acquisition strategy, maintaining contractor oversight and monitoring and updating its acquisition strategy can help TSA ensure that intended results from contracts are achieved as Secure Flight moves forward.

TSA Plans to Develop Oversight Policies and Performance Measures after System Testing

Area of Congressional Interest: Oversight of System Use and Operation

TSA has not yet finalized oversight policies governing the use and operation of Secure Flight or developed performance measures to assess program performance once Secure Flight becomes operational. TSA plans to use Secure Flight's initial testing results to make decisions regarding system data requirements, including the effectiveness of various combinations of PNR data in system operations, and whether the use of commercial data would improve Secure Flight's ability to correctly match PNR data with data contained in the terrorist screening database. TSA officials stated that they plan to use these test results to finalize the Secure Flight concept of operations, which will detail how Secure Flight will operate and interface with other systems. Until this concept of operations is finalized, oversight policies governing the use and operation of the system will not be known. TSA expects to finalize the concept of operations by March 2005.

TSA has also not yet established performance goals or measures to gauge the success of the Secure Flight program once it is operational. Performance goals and measures are intended to provide Congress and agency management with information to be able to systematically assess a program's strengths, weaknesses, and performance, and then identify appropriate remedies. The Government Performance and Results Act requires that agencies establish performance goals and performance measures in order to report on program results.[45] As defined by the act, a performance goal is the target level of performance—either output or outcome—expressed as a tangible, measurable objective, against which actual achievement will be compared. Until Secure Flight testing is complete and key policy decisions are made, such as what data elements will be required in the PNR and whether commercial data will be used, TSA will not be able to finalize performance goals and measures for

[45] Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285.

Secure Flight in an operational environment. However, without performance goals and measures, it will be difficult to determine whether Secure Flight is meeting its objectives. TSA officials stated that while they recognize the need for performance goals and measures for Secure Flight once it is operational, they have not yet identified how or when they will be developed. Until operating policies and performance goals and measures are developed, it is unknown whether needed controls will be put in place to guide and monitor Secure Flight operations.

Although TSA has not developed policies or performance measures for an operational system, it has developed measures for PNR testing and commercial data testing, to identify information on what data combinations are most useful in prescreening passengers and to determine the utility of using commercial data to support Secure Flight operations. For example, TSA developed initial measures for commercial data testing that it plans to refine throughout system testing, should TSA decide to use commercial data. These measures are designed to help determine the effectiveness of using commercial data, and to guide DHS and TSA policy decisions regarding whether the data should be used for the Secure Flight program. Although these measures, and measures developed for PNR testing, were not designed to identify impacts on aviation security in an operational environment, they should help provide TSA a means by which to make informed policy decisions regarding system requirements prior to finalizing its concept of operations.

TSA Has Engaged in Outreach with Key External Stakeholders, but Concerns Exist over Potential Impacts of Secure Flight Operational Requirements

TSA officials have engaged in outreach with key external stakeholders whom they identified as integral to the successful implementation and operations of Secure Flight. However, officials from many of these organizations, primarily air carriers and privacy groups, expressed concerns regarding the uncertainty of Secure Flight system and data requirements, and the impact these requirements may have on the airline industry and traveling public. Officials from a majority of air carriers and privacy groups who answered our questions regarding the implementation of Secure Flight, and who provided comments on the amount of TSA coordination, were generally satisfied with the level of outreach provided related to Secure Flight. However, officials from a majority of the air carriers who provided written comments expressed concern regarding the potential for costly and time-consuming changes that may be required of their reservation systems because of additional data requirements, and the uncertainties surrounding Secure Flight's ability to establish a link for the transfer of data between the air carriers and TSA.[46] Privacy group officials also expressed concerns regarding the integrity of data contained in the terrorist screening database, and the potential lack of a redress process for Secure Flight that would allow a system of recourse for passengers who were misidentified during system screening. TSA officials stated that they will not be able to finalize system requirements until after the completion of initial Secure Flight testing. However, officials identified potential adjustments to reservation systems, and the establishment of a connection with air carriers, as program risks, and are in the process of developing risk mitigation strategies.

TSA Has Discussed Secure Flight Development Activities with Key External Stakeholders

TSA has established relationships with numerous stakeholders—outside of the federal government—that will be involved with, or affected by, the Secure Flight program. These stakeholders include, but are not limited to, air carriers; global reservation management companies; aviation associations; and civil liberties, privacy, and policy advocacy groups. TSA stated that the success of Secure Flight is dependent on building trusted relationships with these stakeholders in order to leverage needed cooperation between the public and the private sector. For instance, TSA officials indicated that the ability of Secure Flight to receive passenger PNR data from air carriers is critical to the operation of the system and that in order to support Secure Flight requirements, the airline industry may need to change its data collection requirements for passengers when reservations are made. TSA also recognized that the protection of passengers' identifiable information is essential for Secure Flight to be successful, since the government will be obtaining, from air carriers, these data in order to conduct Secure Flight prescreening.

TSA focused its outreach efforts on air carriers and privacy groups in an attempt to mitigate their concerns about Secure Flight and resolve issues regarding the implementation and operations of the system. According to TSA officials, they generally held two teleconferences a week with officials from air carriers and privacy groups.[47] TSA officials stated that

[46] We interviewed officials from four air carriers and two aviation associations to assess TSA's outreach efforts to the airline industry and to provide industry stakeholders with an opportunity to communicate perspectives about Secure Flight. In addition to conducting interviews, we asked officials from air carriers to provide written responses to questions about the Secure Flight program.

[47] TSA did not identify how many air carriers or privacy groups it met with to discuss Secure Flight.

they selected these air carriers and privacy groups based on each group's ability to inform the development of Secure Flight. In addition, TSA provided air carriers with a dedicated e-mail address to provide them a means by which to ask questions about, and provide comments on, Secure Flight. TSA committed to responding to all questions and comments within 3 days. During our review of TSA outreach efforts, officials from a majority of privacy groups that we interviewed, and air carriers who provided written comments on TSA's level of outreach, stated that they were generally satisfied or pleased with TSA's level of contact with them related to Secure Flight. In addition, officials from 4 large air carriers stated that TSA's outreach effort had improved from what it had been during the development of CAPPS II. Officials from all three of the privacy groups we interviewed also stated that TSA's outreach effort was a positive change compared with the outreach provided during the development of CAPPS II.

Air Carriers and Privacy Groups Are Concerned about System Connectivity and Data Accuracy and Protections

Although air carriers were generally satisfied with the level of outreach provided by TSA, officials from 13 of the 14 air carriers who answered questions on Secure Flight's implementation expressed concerns about modifications that may be required of their reservation systems and the lack of detailed information from TSA regarding Secure Flight system requirements. Specifically, officials stated that they were concerned about "unknown requirements" and the possibility of being required to collect additional PNR data elements, such as date of birth, when taking passenger flight reservations. According to these officials, requiring the collection of additional PNR data from passengers each time a reservation is made, such as date of birth, would require that all reservation systems—including travel agency systems, Internet engines, self-service kiosks at airports, airport check-in counters, departure systems, and PNR storage databases—be modified, which could place a significant strain on the industry. In addition, officials from 6 of the 14 air carriers expressed various concerns related to customer inconvenience, including concerns about the collection of additional information at the check-in or departure gate, potentially resulting in congested airports and delayed departures and possibly creating an increased workload for airline personnel. Officials further stated that passengers could face delays by having to provide additional data when making reservations or during the check-in process at the airport. Officials were unable to provide estimates of potential costs of system changes or expected delays since TSA has not yet defined what data elements Secure Flight will require to conduct passenger prescreening. However, some officials—although uncertain of what the Secure Flight system requirements will be—estimated that it may require anywhere from 8 weeks to over 1 year to make required changes to their reservation systems, depending on data requirements.

Air carrier officials also expressed concern that TSA has not yet developed a plan identifying how connections will be made between air carrier reservation systems and TSA to support Secure Flight prescreening. Officials from 11 of the 14 air carriers who provided written comments expressed various concerns regarding connectivity, including Secure Flight's ability to provide a two-way real-time exchange of data to allow for the almost instantaneous prescreening of passengers. Officials further stated that the maximum load capacity of systems that may be used to transfer data between the air carriers and TSA, such as the Advanced Passenger Information System, may not be sufficient to handle the large amount of data that will need to be regularly transferred. Air carrier officials also expressed concern that the programming effort needed to establish a two-way connection between their reservation systems and the Advanced Passenger Information System, enabling carriers to both send and receive data almost instantly, would be costly and time-consuming. As we noted earlier, TSA will need to resolve these and additional issues with TSC, which will provide data from the terrorist screening database, and CBP, to receive PNR data, before these connections can be determined.

Although air carrier officials identified concerns related to unknown system requirements, some officials stated that they believed Secure Flight will provide improvements over the current prescreening process, and may provide additional benefits to air carriers and passengers. Specifically, officials from 5 of the 14 air carriers stated that they expect to realize benefits, such as eliminating the air carriers' responsibilities for operating CAPPS I and watch list matching and transitioning the prescreening responsibility to the government. In addition, officials from 2 of the 5 air carriers stated that Secure Flight may result in a more consistent application of procedures. Three officials further stated that transferring the prescreening responsibility to the federal government will eliminate the need for air carriers to maintain terrorist watch list data and to manually process customers, which should result in a reduced workload and operational savings to the air carriers. Officials further stated that Secure Flight may minimize unnecessary delays for passengers who may have been falsely matched against the selectee and no-fly lists, which would have required them to undergo additional security screening.

Privacy group officials we contacted also expressed concern regarding the potential impact of Secure Flight requirements once they are defined, primarily the integrity of data contained in the terrorist screening database and the lack of a Secure Flight redress policy. Although officials from all three privacy groups we contacted recognized that the quality of data contained in the terrorist screening database was outside the control of TSA, they stressed the importance of having established processes for adding individuals to, and removing individuals from, the database to help ensure the accuracy of the data. One official stated that inaccurate data in the terrorist screening database could lead to an increase in the number of individuals being misidentified as positive matches against a terrorist watch list. Officials from all three groups also expressed concern over the lack of a finalized redress process, which would provide passengers who were misidentified as positive matches against data in the terrorist screening database a means by which to correct erroneous information. According to one official, a redress process should incorporate access to information, the ability to challenge a decision, and the identification of the information's source in order to correct the information if necessary. As noted earlier, TSA is in the process of addressing these concerns by establishing a memorandum of understanding with TSC to help ensure the accuracy of data contained in the terrorist screening database, and it is developing a redress policy.

TSA Has Initiated Information System Security Activities but Cannot Complete All Key Actions until Secure Flight Is Further Developed

Area of Congressional Interest: Operational Safeguards and Security Measures

TSA is planning to implement an information systems security management program for Secure Flight, but key elements of this program have not yet been completed, due in part to the status of Secure Flight's development. Although TSA has taken steps to initiate a security risk assessment and a security plan, other steps, such as certification and accreditation, cannot occur until the system has been developed and tested.

The Federal Information Security Management Act,[48] Office of Management and Budget (OMB) guidance,[49] and industry best practices describe critical elements of a comprehensive information system security management program. These elements include conducting a security risk assessment and developing a system security plan, obtaining a security certification, and having an agency official accredit the security of the system. Together, these elements can help provide a strong security

[48] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, §§ 301-305, 116 Stat. 2946, 2946-61.

[49] OMB, *Management of Federal Information Resources*, Office of Management and Budget Circular A-130.

framework for protecting information and assets. A comprehensive information system security management program can, among other benefits, help ensure 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.

In part because Secure Flight has not yet been fully defined or developed, TSA has not yet completed a security risk assessment and a security plan. Risk assessments are essential steps in determining what controls are required and what level of resources should be expended on controls, while 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. TSA has drafted a risk assessment for Secure Flight and the Transportation Vetting Platform. TSA also developed a draft security plan that references the high-level system controls needed for security, including management, operational, and technical controls. However, greater detail regarding the specific steps to be taken to secure the system will be needed before the plan can be finalized. For example, the security plan should include details about security controls associated not only with the Secure Flight program but also its many interfaces and networks that are to provide connectivity to the carriers. TSA estimates that it will complete the risk assessment and security plan by April 2005.

Furthermore, since Secure Flight requirements have not been fully defined and the system is still undergoing development and testing, TSA is unable to certify and accredit the system as secure. Certifying and accrediting a system as secure requires that the appropriate officials have the necessary information to make a credible risk-based decision regarding whether to put the system into operation. This process is typically completed after the system is fully developed. Identifying and assessing information security risks and developing system security plans are two critical activities that directly support security accreditation. TSA estimates that it will obtain system certification and accreditation by July 2005.

Although TSA plans to implement a security management program for Secure Flight, TSA officials acknowledged that information security is a key risk area. To mitigate a possible risk of not certifying and accrediting the Secure Flight system on schedule, TSA officials stated that the Office of Transportation Vetting and Credentialing would apply resources to these security issues—within a minimum of 4 months prior to the planned operational date—to provide time to meet the certification and accreditation requirements. TSA initially projected that Secure Flight would be certified and accredited by January 2005 based upon key development and testing milestones. However, these milestones have since slipped to July 2005 to align with system readiness.

TSA acknowledged that completion of the security risk assessment, system security plan, and certification and accreditation process is critical to ensuring the security of Secure Flight. DHS Management Directive 4300 requires that these be completed before the system can become fully operational. TSA has developed a schedule to accomplish these activities. Failure to complete the comprehensive risk assessment and security plan on schedule, however, could result in an increased risk that the system certification and accreditation may be delayed.

Life-Cycle Cost Estimates Have Not Been Developed and An Expenditure Plan Was Recently Finalized

Area of Congressional Interest: Life-Cycle Cost Estimates and Expenditure Plans

TSA's life-cycle cost estimates have not been developed, in part because key decisions regarding how Secure Flight will operate, and the data it will use, have not yet been made. TSA also recently finalized an expenditure plan detailing plans for future program expenditures. Life-cycle cost estimates and expenditure plans are critical components of sound program management for the development of any major investment. Developing life-cycle cost estimates also reflects Office of Management and Budget guidance and can be important in making realistic decisions about developing a system.[50] Expenditure plans, which generally identify near-term spending, are designed to provide lawmakers and other officials overseeing a program's development with a sufficient understanding of the system acquisition to permit effective oversight, and to allow for informed decision making about the use of appropriated funds.

TSA officials stated that they have not yet developed reliable life-cycle cost estimates for the Secure Flight program because of the uncertainties surrounding Secure Flight's requirements, such as whether commercial data will be used. Life-cycle costs represent the overall estimated cost for a particular investment alternative over a period of time corresponding to the life of the investment, including initial direct and indirect costs plus any periodic or continuing costs of operation and maintenance. According to TSA officials, life-cycle cost estimates cannot be accurately developed until after initial testing has taken place and policy decisions have been made regarding Secure Flight requirements. For example, TSA officials

[50] OMB, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, Office of Management and Budget Circular A-11, Part 7 (July 2002).

stated that the estimated cost to operate Secure Flight can more accurately be made after TSA has decided whether to use commercial data to verify a person's identity as part of the program. According to TSA officials, the use of commercial data could greatly increase the annual cost to operate the Secure Flight program. TSA has also not determined the cost associated with obtaining system connectivity, such as developing an interface between CBP and air carriers in order to transmit data. Because of these uncertain program requirements, TSA considers life-cycle costs to be a key risk facing Secure Flight.

While TSA believes it cannot provide reliable cost estimates at this point in the development of Secure Flight, TSA should be able to develop initial estimates of life-cycle cost ranges for Secure Flight, using certain assumptions about the program's components. Life-cycle cost estimates can include a cost range based on certain factors. For example, the high-end estimate would assume the most expensive operating cost possible for the system (if all components being considered were incorporated), and the low-end estimate would assume the least expensive operating cost (if all components being considered were not incorporated). However, TSA officials stated that they will not develop life-cycle costs until after testing is complete and policy decisions have been made regarding program requirements. Officials could not identify a date when they expect these estimates to be developed.

Moreover, estimating life-cycle costs is an important oversight procedure for a program. A reliable life-cycle cost estimate can be important in making realistic decisions about developing a system, and can alert an agency to growing cost problems and the need for mitigating actions. Accordingly, reliable life-cycle cost estimates should be developed as early in the program's development as possible. Failure to develop reliable life-cycle cost estimates could increase the risk that a program may be underfunded and subject to cost overruns, which could result in a program being reduced in scope or additional funding being requested and appropriated to ensure the program meets its objectives. Conversely, overestimating life-cycle costs creates the risk that a program will be deemed unaffordable. As TSA moves forward with the development and implementation of Secure Flight, it will be important for TSA to follow guidance issued by the OMB in developing life-cycle cost estimates.

TSA recently finalized its Secure Flight expenditure plan, which TSA refers to as a spend plan, for its fiscal year 2005 appropriation.[51] According to TSA officials, this plan includes planned expenses for each month in fiscal 2005 for each major program, project, or activity, such as government personnel-related costs; communications, including information technology; and other contractual services. Because TSA had only recently finalized the expenditure plan, it was not available for our review. However, our experience in working with Congress and other agencies in developing and implementing expenditure plans shows that these plans need to disclose a sufficient level and scope of information for oversight officials to understand what system capabilities and benefits are to be delivered, by when, and at what cost, and what progress is being made against the commitments that were made in prior expenditure plans.[52] Further, expenditure plans should disclose how the program will be managed to provide reasonable assurance that system capability, benefit, schedule, and cost commitments will be met. TSA's expenditure plan should include this level of detail in order to provide the Congress with the information needed for effective oversight.

[51] TSA uses the term *expenditure statement* to refer to its record of funds that have been spent.

[52] GAO, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (Washington, D.C.: June 9, 2003).

TSA Has Taken Steps to Minimize Impacts on Passengers and Protect Passenger Rights, but Its Operational Plans Must Be More Fully Defined before Protections and Impacts Can Be Accurately Assessed

The data-matching functionality planned for Secure Flight, which TSA is in the process of testing, involves accessing and manipulating personal information about travelers and thus has the inherent potential to adversely affect their privacy or impact their rights. Aware of this potential, TSA has begun to take steps to minimize potential impacts and protect passenger rights. However, TSA has not yet clearly defined the privacy impacts of the planned system or the full actions it plans to take to mitigate them. For example, although TSA developed documentation identifying potential privacy impacts for Secure Flight data processing tests, it has not yet assessed the potential impact on passenger privacy of the system in an operational environment, because of the early stage of Secure Flight's development. TSA has also drafted a redress process to provide passengers who believe they were inappropriately delayed from boarding their scheduled flights because of Secure Flight a means by which to appeal these decisions. However, TSA has not yet clearly defined how it plans to implement this process. According to TSA, the draft Secure Flight redress process is similar to the current process for addressing passenger complaints about the watch list screening process, but differs in that it will provide individuals who believe they have been inappropriately selected for secondary screening the opportunity to seek redress. Further, in order to provide redress with respect to the terrorist screening database, agreements must be reached with other key stakeholders. These agreements have not yet been reached, adding to the uncertainty about how the operational system may affect passengers and whether the redress process will be an improvement over what is currently in place. In addition, although DHS and TSA have taken steps to address international privacy concerns in developing Secure Flight, such as limiting Secure Flight to prescreening only domestic passengers, issues remain, particularly with regard to the European Union. Until TSA fully defines its operational plans for the Secure Flight system—which officials stated they plan to do later in the system's development—it will remain difficult to determine whether the planned system will offer reasonable privacy protection to passengers who are subject to prescreening or mitigate potential impacts on passengers' privacy.

Privacy Protections and Impacts Cannot Yet Be Assessed

Area of Congressional Interest: Privacy Concerns

The Privacy Act—the primary legislation that regulates the government's use of personal information[53] —requires that agencies maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency.[54] However, it is difficult to determine whether Secure Flight will meet this requirement because TSA has not determined what personal information will be maintained in the system. TSA officials stated that the purpose of recently completed Secure Flight testing was to determine what information from PNRs was relevant and necessary to support Secure Flight operations. TSA officials further stated that during testing, they planned to determine whether additional data elements, such as date of birth, would be necessary to match PNR data against data in the terrorist screening database. Until TSA determines which data elements will be required for Secure Flight operations, based on the results of these tests, whether TSA is collecting only relevant and necessary personal information cannot be determined.

The Privacy Act also requires agencies to publicly release specific information regarding the handling of privacy-related information in systems that contain such information. On September 21, 2004, TSA released privacy notices for the Secure Flight data processing test. These notices included a privacy impact assessment, system of records notice, proposed information collection request, and a proposed order to airlines to provide PNR data.[55] In the system of records notice, TSA claimed several exemptions from Privacy Act requirements for the test.[56] However, to date, TSA has not published a rule explaining the reasons for these

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

[54] See 5 U.S.C. § 552a(e)(1).

[55] The E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain, or disseminate information in an identifiable form. Further, the Privacy Act requires that an agency publish a system of records notice in the *Federal Register* upon establishment or revision of the existence and character of any system of records. The system of records notice is to include information such as the name and location of the system, and "routine uses" of the records contained in the system. Under the Paperwork Reduction Act of 1995, Pub. L. 104-13, 109 Stat. 163, agencies must submit to the Office of Management and Budget for approval an information collection request, which in this case was the proposed order to the airlines to provide passenger name records.

[56] Portions of the system of records being tested were claimed to be exempt from 5 U.S.C. § 552a(c)(3),(d), (e)(1), (e)(4)(G) and (H), and (f) pursuant to 5 U.S.C. § 552a(k)(1) and (k)(2).

exemptions, as required by the Privacy Act.[57] TSA officials stated that they subsequently decided not to claim Privacy Act exemptions and, therefore, did not need to issue a rule. According to TSA officials, they made their decision based on TSA's confidence in its ability to control access to the information pursuant to other legal authority. On March 14, 2005, TSA officials stated that they intend to issue a revised system of records notice reflecting their decision not to claim Privacy Act exemptions. Further, they stated that an additional set of privacy notices would be issued once the data processing test was complete and results had been analyzed, and that they intended to issue a Privacy Act exemption rule for the operational phase of the program that would implement any exemptions claimed and explain the agency's basis for claiming such exemptions. TSA officials stated that they plan to issue a draft rule and privacy notices for Office of Management and Budget review in May 2005, and a final rule and privacy package in June 2005. A determination of whether Secure Flight will be in compliance with the Privacy Act cannot be made until such notices are issued.

Privacy is also a consideration within the broader context of Fair Information Practices—a set of internationally recognized privacy principles that underlie the Privacy Act.[58] As with the Privacy Act, given the stage of Secure Flight's development, it cannot yet be determined whether Secure Flight will adhere to the Fair Information Practices. For example, one of the Fair Information Practices is 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. However, as we have noted, potential concerns exist regarding reliance on the terrorist screening database that is outside the scope of TSA's control, and regarding how passengers will be able to access and correct erroneous information. In addition, although TSA required that airlines provide all information from designated PNRs for its data processing test, TSA will need to make an explicit determination about what data elements from the

[57] See 5 U.S.C. § 552a(k). According to OMB guidance, "upon determining that a system is to be exempted under this section, the agency head is required to publish that determination as a rule under the Administrative Procedure Act, subject to public comment." 40 Fed. Reg. 28,948, 28,972 (July 9, 1975).

[58] 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. These practices are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation, and accountability.

PNR or other data it plans to collect in order for the operational system to comply with the “relevant and necessary” standard. Whether TSA will collect only relevant and necessary personal information cannot be assessed until this determination is made. For example, TSA officials acknowledged that they still have to reach agreements with TSC regarding the information TSA plans to receive from TSC, including data quality requirements and the correction of erroneous information contained in the terrorist screening database, and they stated that they are in the process of negotiating this agreement. Further, TSA’s plans to test the use of commercial data include consideration of the possible use of such data to augment airline-provided PNR data. According to TSA officials, they plan to define the final redress process in April 2005 and issue a final privacy rule and notices in June 2005.

A Redress Process Is Being Developed, but Key Stakeholder Roles and Responsibilities Have Not Yet Been Defined

Area of Congressional Interest: Redress Process

A robust redress process is key to protecting passenger rights because it establishes a system of due process whereby aviation passengers who believe they have been inappropriately delayed from boarding their scheduled flights by TSA may appeal such decisions and correct any erroneous underlying information contained in the Secure Flight system. A robust redress system would address the Privacy Act’s requirement that individuals be able to access and correct their personal information. It is also fundamental to the Fair Information Practice known as individual participation—the ability of individuals to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.

Under the current passenger prescreening system, air carriers compare passenger information against no-fly and selectee lists provided by TSA. The comparison of passenger information against the no-fly and selectee lists can result in passengers being unnecessarily delayed or denied boarding should they have a name that is the same as, or similar to, that of a person on a watch list. To address this issue within the current system, TSA developed a clearance procedure whereby passengers who experience delays may submit a passenger identity verification form to TSA for a determination about whether the passenger is to be placed on a “cleared” list. If upon review, TSA determines that the passenger’s identity is distinct from the person on a watch list, TSA is to notify the airlines and notify the passenger that, in the future, the clearance procedure will aid in expediting the person’s check-in process. However, the effectiveness of the current redress process is uncertain. For example, TSA officials stated that the process currently in place does not provide redress for those who are included on a watch list but who believe such inclusion is inappropriate.[59]

According to TSA officials, the redress process envisioned for Secure Flight will be based on the current process, with two major extensions. First, individuals who believe they have been inappropriately included in the terrorist screening database are to have the opportunity to seek redress. While exact implementation details remain undetermined, TSA officials said they plan on establishing an agreement with TSC to review the reasons for an individual being in the terrorist screening database should that individual seek redress. According to this concept, TSC would assess the reason a person is listed in the database, including consulting with the originating agency, and would remove a person from the database if appropriate. Second, the Secure Flight redress process is to include an appeals process—a feature also not available under the redress process. According to TSA officials, although the criteria to be used for handling redress cases is under development, the Secure Flight redress process would allow passengers to file a first-level appeal with the TSA Privacy Officer or the Director of Civil Rights if discrimination is alleged, and, if necessary, a second-level appeal with the DHS Privacy Officer.

Like the current redress process, the proposed Secure Flight redress process would be initiated by a passenger registering a compliant with TSA. After receiving a completed passenger identity verification form from the complainant, TSA is to investigate the cause behind the screening decision. If the cause is a name similarity (false positive) or an exact match with the terrorist screening database, TSA is to refer the case to TSC for further investigation—not a feature of the current redress process. While TSA and TSC have not reached an agreement related to Secure Flight, the system's draft redress process states that TSC will review screening decisions, including verification of any match, review of intelligence information, and consultation with originating intelligence agencies. The resolution of these reviews, including responsibilities for adjudication of different views and information, remains to be determined. Additionally, it remains unclear whether the appeals process will provide passengers with the ability to appeal determinations made by the TSC.

[59] TSA officials stated that under the current process, they reviewed the reasons three or four individuals were included on the watch list. However, the current redress process does not contain formal provisions for this review.

Ensuring that the proposed redress process for Secure Flight is robust will be challenging for TSA for two significant reasons. First, much of the information underlying decisions to add individuals to the TSC terrorist screening database is likely to be classified, and as such, it will not be accessible to passengers, who will inevitably face substantial restrictions on their ability to know what information is being associated with them, as is the case with the current process. Second, TSA does not control the content of the terrorist screening database that it intends to use as the primary input in making screening decisions, and will have to reach a detailed agreement with the TSC outlining a process for correcting erroneous information in the terrorist screening database. Until TSA and TSC reach an agreement, it will remain difficult to determine whether redress under Secure Flight will be an improvement over the process currently used or if it will provide passengers with a reasonable opportunity to challenge and correct erroneous information contained in the system.

In addition, although still in draft, TSA's concept for redress focuses on individuals inconvenienced by the system—persons "singled out too frequently." The draft redress process documentation does not address a means for passengers who are inappropriately denied boarding to seek redress. A robust redress process should not only alleviate the annoyance of repeated additional screening, but should also provide redress to those who are wrongfully denied boarding. TSA will need to fully define how to handle redress for those denied boarding as it develops the redress process for Secure Flight.

At the time of our review, TSA had not yet decided whether Secure Flight would use commercial data to assist in reducing false positives, identifying false negatives, and verifying the validity of the identities presented by passengers. However, should TSA decide to proceed with the use of commercial data, it will need to address several concerns. First, since TSA does not control the content of commercial databases, it will need to reach specific agreements with commercial data aggregators on a process for correcting erroneous information. We previously reported that under CAPPS II, TSA proposed that it would be the responsibility of passengers to contact the owners of commercial databases directly in order to correct inaccurate information.[60] However, correcting such erroneous information may be difficult because commercial data providers, which aggregate data

[60] GAO-04-385.

from other sources, may have no obligation to correct the data they maintain. Further, the exact source of commercial data used in any given screening decision might not be disclosed to the passenger, because of licensing agreements. Should TSA proceed with using commercial identity verification, it will need to address these concerns and reach specific agreements with commercial data aggregators similar to the agreement it will need to reach with TSC.

Secure Flight Design Reduces Some International Privacy Concerns, but Issues Remain

As noted in our February 2004 report on CAPPS II, obtaining international cooperation to obtain passenger data to prescreen international passengers for CAPPS II was a significant challenge.[61] In order to provide prescreening of passengers on international flights in addition to domestic flights, CAPPS II needed data on passengers from foreign countries, flying on foreign airlines, or purchasing tickets through foreign sources. However, the European Union, in particular, raised concerns about its citizens' data being used by CAPPS II, asserting that using such data is not in compliance with its privacy directive. At the end of 2003, DHS and European Union officials finalized an agreement regarding the transfer of data for use by CBP that would permit TSA to use European Union passenger data for testing CAPPS II. The agreement, however, did not permit TSA to use these data for CAPPS II operations. According to European Union officials, they were prepared to discuss the use of these data in a second, later round of negotiations when U.S. governmental processes were complete and congressional concerns about privacy protections were addressed.

TSA officials stated they have been sensitive to European Union privacy concerns in developing Secure Flight and have taken steps to address these concerns. Specifically, TSA officials stated that Secure Flight will only screen passengers on domestic flights. Passengers on international flights will continue to be screened by CBP. TSA also agreed that the agreement to permit the use of European Union data for CAPPS II testing does not apply to Secure Flight. Further, in its order requiring airlines to provide historical PNR data for Secure Flight testing, TSA allowed air carriers to exclude from the June 2004 PNR submission any European Union flight segments. According to TSA officials, this provision was designed to help the air carriers avoid any potential liability that could arise from providing European Union passenger data for Secure Flight

[61] GAO-04-385.

testing, while making clear that TSA has statutory authority to prescreen European Union citizens on U.S. domestic flights.[62] Nonetheless, TSA has acknowledged that the use of passenger data that originates in reservations made in a European Union country may create concerns under that country's privacy laws. For example, European Union privacy laws cover personal information originating in the European Union. Thus, even a wholly domestic U.S. flight could involve European Union data if the passenger purchased the ticket in the European Union. Further, because TSA and CBP have not finalized plans for how CBP will transmit airline passenger data (PNRs) to TSA for Secure Flight, it has not been decided whether CBP or TSA will filter out international passenger data before the PNRs are inputted into Secure Flight. If TSA performs this filtering of international passenger data, additional questions may be raised about TSA handling personal data of individuals from the European Union and other countries. According to TSA officials, they are working toward both a political and a technical solution to these issues. DHS and TSA officials further stated that they briefed European Union officials of plans for Secure Flight and would continue regular discussions to keep them apprised of Secure Flight development. According to TSA officials, there is no indication of significant concerns with Secure Flight from any other nations.

Conclusions

TSA is making progress in addressing key areas of congressional interest related to the development and testing, system effectiveness, program management and oversight, and privacy protections for the Secure Flight program, as outlined in Public Law 108-334. Specifically, TSA is in various stages of addressing each of the 10 areas of interest outlined in the law, including establishing a framework for a redress process; beginning testing to measure the effectiveness of system data matches; and using oversight boards to oversee the development of Secure Flight. However, TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the system's development. Specifically, initial system testing has only recently been completed, and key policy decisions—including what data will be collected and how they will be transmitted—have not yet been made. Until requirements are defined and testing is completed, and operating policies are finalized—scheduled for

[62] TSA did not require the air carriers to exclude these segments because of concerns over the cost and time constraints imposed on the air carriers in providing the data. Because not all air carriers were able to separate passenger data from European Union flight segments, TSA officials stated that they excluded these segments when designing their tests.

later in the system's development—we cannot determine whether Secure Flight, in an operational environment, will fully address these areas of interest.

As development and testing of Secure Flight continue, and program policy decisions are made, TSA will need to manage key program risks in order to help ensure the system meets its intended objectives as it becomes operational. A key program risk is related to requirements definition and system testing. TSA has made progress in recently completing initial testing for Secure Flight. However, TSA has not finalized its system requirements or concept of operations, or developed detailed test plans for critical system testing. Until TSA finalizes these documents and completes additional system testing, it is uncertain how well Secure Flight will perform, or whether it will be ready for operational deployment in August 2005. It will be important for TSA to effectively manage the system changes that are likely to result from the final testing phases with sound management discipline and rigor.

Another key program risk is the ability of TSA to establish connectivity between air carrier reservation systems and TSA to allow for the transmission of data to support Secure Flight operations. TSA officials have not yet developed a plan identifying how connections will be made between air carrier reservation systems and TSA to support Secure Flight prescreening. The majority of air carrier officials we interviewed expressed various concerns regarding connectivity, including Secure Flight's ability to provide a two-way real-time exchange of data to allow for the almost instantaneous prescreening of passengers. Further, officials from TSA and CBP stated that it was uncertain whether CBP's existing systems—which will support the transfer of data—will be able to handle the large amount of data that will need to be regularly transferred. The effectiveness of Secure Flight in obtaining the data it needs to make accurate matches against the terrorist screening database, and to transmit the results of data matches to air carriers in a timely manner, is directly affected by the system's ability to send and receive data. Moreover, key decisions on how connectivity will be established could affect the cost, schedule, and performance of Secure Flight.

Ensuring that impacts on passengers are minimized, and passenger rights are protected, is also critical to the success of Secure Flight. Concerns over privacy protections related to Secure Flight's predecessor, CAPPS II, led—in part—to an internal departmental review of the program and its ultimate cancellation. TSA has begun to take steps to minimize potential impacts on passengers and to protect passenger rights during the initial testing phase of Secure Flight, including releasing privacy notices for Secure Flight data processing tests. However, TSA has not yet clearly defined privacy impacts of Secure Flight in an operational environment, or the full actions it plans to take to mitigate potential impacts, due in part to the current stage of the system's development. For example, TSA does not plan to determine whether additional data elements will be necessary to match passenger data to data contained in the terrorist screening database until further testing is completed. Until TSA determines which data elements will be required, based on the results of testing, it is unclear whether TSA will collect only relevant and necessary personal information for Secure Flight. Further, although TSA developed a conceptual description of its planned redress process for Secure Flight, key elements of this process are still being determined, including agreements with key stakeholders, such as TSC. Ensuring that a robust redress process is developed for Secure Flight will be challenging, since much of the information underlying decisions to add individuals to the terrorist screening database is likely to be classified, and may not be easily accessed and corrected.

Additionally, TSA has not yet developed performance goals and measures to gauge the effectiveness of the Secure Flight program, once it becomes operational. Performance goals and measures are intended to provide Congress and agency management the ability to systematically assess a program's strengths, weaknesses, and performance, and then identify appropriate remedies. Performance goals and measures can assist TSA in determining whether Secure Flight, once operational, achieves its intended results. TSA also has not developed life-cycle cost estimates and only recently finalized an expenditure plan, which are key steps in providing those with oversight responsibilities with information needed to make informed decisions. Life-cycle cost estimates should be developed as early in a program's development as possible. Failure to develop reliable estimates can increase the risk that a program may be underfunded and subject to cost overruns, or will not be affordable. Further, expenditure plans should be developed to include a sufficient level of detail to identify what system capabilities will be delivered, by when, and at what cost. In addition to providing system development and contractor oversight, TSA will need to develop and finalize these estimates and plans to help ensure sound program management and oversight.

Recommendations for Executive Action

To help manage risks associated with Secure Flight's continued development and implementation, and to assist the Transportation Security Administration in developing a framework from which to support its efforts in addressing congressional areas of interest outlined in Public Law 108-334, we recommend that the Secretary of the Department of Homeland Security direct the Assistant Secretary, Transportation Security Administration, to take the following six actions:

- Finalize the system requirements document and the concept of operations, and develop detailed test plans to help ensure that all Secure Flight system functionality is properly tested and evaluated. These system documents should address all system functionality and include system stress test requirements.

- Develop a plan for establishing connectivity among the air carriers, U.S. Customs and Border Protection, and the Transportation Security Administration to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations.

- Develop reliable life-cycle cost estimates and expenditure plans for Secure Flight—in accordance with guidance issued by the Office of Management and Budget—to provide program managers and oversight officials with information needed to make informed decisions regarding program development and resource allocations.

- Develop results-oriented performance goals and measures to evaluate the effectiveness of Secure Flight in achieving intended results in an operational environment—as outlined in the Government Performance and Results Act—including measures to assess associated impacts on aviation security.

- Prior to achieving initial operational capability, finalize policies and issue associated documentation specifying how the Secure Flight program will protect personal privacy, including addressing how the program will comply with the requirements of the Privacy Act of 1974 and related legislation.

- Prior to achieving initial operational capability, finalize policies and procedures detailing the Secure Flight passenger redress process, including defining the appeal rights of passengers and their ability to access and correct personal data.

Agency Comments and Our Evaluation

We provided a draft copy of this report to DHS for its review and comment. On March 22, 2005, we received written comments on the draft report, which are reproduced in full in appendix II. DHS generally agreed with the report and recommendations, and described some actions it has initiated to address the recommendations. DHS further stated that initial system testing demonstrated that needed functionality is in place to support program implementation. DHS also provided technical comments related to the program's development, testing, and implementation. These comments were incorporated as appropriate.

Regarding actions DHS reported taking to address the recommendations, DHS stated that TSA plans to complete the Secure Flight concept of operations by March 2005, and system requirements by April 2005. DHS also noted that formal arrangements between CBP and TSA and for two-way connectivity with air carriers are in progress. DHS also acknowledged that while they plan to prepare life-cycle costs and a comprehensive set of critical performance measures for Secure Flight, these efforts will be accomplished during the later stages of the system's development. DHS further stated that TSA will issue for public comment a new privacy package as it implements Secure Flight, and is finalizing a redress process for passengers who feel they have been unfairly or incorrectly singled out for additional screening.

DHS also highlighted several key TSA achievements, including issuing a privacy package for Secure Flight testing, awarding a contract for testing, developing an acquisition plan, and working jointly with the TSC and CBP to prepare a draft concept of operations. DHS further expressed concern that the report did not appropriately characterize the status of the system's development and testing. Specifically, DHS stated that recently completed functionality testing confirmed TSA's key hypotheses about Secure Flight's data matching capabilities, and demonstrated that the needed functionality exists to support the implementation of Secure Flight. We recognized that TSA recently reported completing testing of key data matching functions, and that it believes this testing confirmed its hypotheses and demonstrated some functionality. However, because this testing was only recently completed and test results have not been fully documented and analyzed, we were unable to independently assess these results. In addition, TSA did not test all of the functions planned for Secure Flight, such as the connectivity needed to obtain and match data from the air carriers with data in the terrorist screening database. The testing of this function and other key functions is scheduled to occur during the final phases of testing. In fact, TSA plans to begin a full range of unit, integration, system, stress testing, and end-to-end testing in April 2005. Thus, while we acknowledge that TSA completed important initial testing of system functionality, critical system testing has not yet been conducted. These tests are needed to determine whether Secure Flight will provide the desired functionality and operate as intended in an operational environment.

In addition, DHS highlighted that TSA had issued a comprehensive privacy package for Secure Flight testing and, in response to our recommendation that TSA finalize how it will comply with the Privacy Act, DHS stated that TSA is currently in compliance with the Privacy Act. However, as discussed in the report, the Privacy Act requires TSA to publish a rule explaining the reasons for the exemptions it claimed in its system of records notice, issued in September 2004. To date, TSA has not published such a rule. In a discussion with us on March 14, 2005, TSA officials stated they no longer wish to claim an exemption from the Privacy Act and that they intend to issue a revised system of records notice that would serve to notify the public of this change. TSA has not yet published a revised notice, and DHS official comments to a draft of this report do not refer to plans for a revised notice. Until TSA either publishes the rule required by the Privacy Act or issues a revised system of records notice, it will not be fully compliant with the Privacy Act with regard to the test phase of the program. Further, as identified in the report, TSA will have to comply with the Privacy Act for Secure Flight beyond the testing phase once the system becomes operational.

We are sending copies of this report to the Secretary of the Department of Homeland Security, the Administrator of the Transportation Security Administration, and the Assistant Administrator of the Office of Transportation Vetting and Credentialing. 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 berrickc@gao.gov, or Christine Fossett, Assistant Director, at (202) 512-2956, or fossettc@gao.gov. Questions concerning system development and testing or security should be directed to David Powner at (202) 512-9286, or pownerd@gao.gov. Major contributors to this report are listed in appendix III.

Cathleen A. Berrick

Cathleen A. Berrick
Director, Homeland Security
and Justice Issues

David A. Pow

David A. Powner
Director, Information Technology
Management Issues

List of Congressional Committees

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

The Honorable Ted Stevens
Chairman
The Honorable Daniel K. Inouye
Ranking Minority Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Jerry Lewis
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 Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
House of Representatives

Appendix I: Objectives, Scope, and Methodology

To assess efforts by the Transportation Security Administration (TSA) to develop and implement Secure Flight as mandated by Public Law 108-334, enacted in October 2004,[1] we addressed the following four questions: (1) What is the status of Secure Flight's development and implementation? (2) What factors could influence the effectiveness of Secure Flight? (3) What procedures have been put in place to oversee and manage the Secure Flight program, including ensuring stakeholder coordination? And (4) What efforts are being taken to minimize the impacts on passengers and protect passenger rights? In addressing these four questions, we also addressed the 10 specific issues that we were mandated to review under Public Law 108-334. Since some of the information addressing the congressional areas of interest is considered Sensitive Security Information, we are also issuing a separate letter containing this information.

To determine the status of Secure Flight's development and implementation, we interviewed officials from the TSA's Office of Transportation Vetting and Credentialing—the Office of National Risk Assessment prior to November 2005—which is responsible for developing and implementing Secure Flight, and the Office of Aviation Operations. We also reviewed program documentation including Secure Flight system requirements, a draft concept of operations, test plans, a project schedule, and a working milestone chart. We also reviewed a summary of TSA's preliminary Secure Flight test results. In addition, we traced existing test results to Secure Flight system requirements to determine the completeness of Secure Flight testing. We interviewed testing officials to discuss test activities and results and plans for future testing. We also obtained information on requirements and testing of the computer-assisted passenger prescreening system (CAPPS II) and obtained additional information regarding the differences and similarities between the current computer-assisted passenger prescreening system (CAPPS I), CAPPS II, and Secure Flight. We reviewed relevant legislation as it pertained to Secure Flight. Further, in determining the status of Secure Flight's development and implementation, we addressed the mandated issue identified in Public Law 108-334 related to TSA's efforts to stress test all search tools in Secure Flight and demonstrate that the system can make accurate predictive assessments of passengers who might constitute a threat to aviation.

[1] Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, § 522, 118 Stat. 1298, 1319-20 (2004).

To address our second objective, related to factors that could influence the effectiveness of Secure Flight, we interviewed officials from TSA's Office of Transportation Vetting and Credentialing and TSA's Office of Aviation Operations. We also interviewed officials from the U.S. Customs and Border Protection and the Terrorist Screening Center, which are key stakeholders for Secure Flight. We reviewed program documentation, including Secure Flight system requirements, a draft concept of operations, test plans, and test results, as available. We interviewed TSA officials regarding their recently completed tests designed to identify the most effective combination of data elements in air carriers' passenger name records (PNR) and the terrorist screening database to be matched. We discussed the testing and analysis conducted and reviewed a summary of the initial test results, because the test data and final reports were not yet available for our review. We also discussed issues relating to the commercial data test with TSA officials. We interviewed officials associated with the Terrorist Screening Center, which is responsible for the development and maintenance of the terrorist screening database, regarding their process for placing names on and removing names from the database and the methods used to ensure the accuracy of the database. However, we did not independently verify the procedures used. We also reviewed recent changes to the CAPPS I rules and interviewed TSA officials to determine modifications that have been made to the system to accommodate intrastate transportation in states with unique needs. In addition, we interviewed TSA officials and reviewed documents regarding the ability of Secure Flight to identify passengers who assume the identity of another individual, known as identity theft. In determining what factors could influence the effectiveness of Secure Flight, we addressed the mandated issues identified in Public Law 108-334 related to TSA's efforts (1) to ensure that the underlying error rate of the databases that will be used will not result in a large number of false positives, and (2) to modify Secure Flight with respect to intrastate transportation to accommodate states with unique needs and passengers who might otherwise regularly trigger selectee status.

To address our third objective, regarding determining the processes and procedures in place to oversee and manage the Secure Flight program, including stakeholder coordination, we interviewed officials from the Office of Transportation Vetting and Credentialing and other TSA and DHS officials with Secure Flight oversight and management responsibilities. We reviewed documentation on internal and external oversight mechanisms, including documents submitted to DHS's Investment Review Board and the board's decision, the draft business case for the Transportation Vetting Platform, and documents related to the Aviation Security Advisory

Committee working group focusing on Secure Flight. We also reviewed documentation on program management—contract and security management, performance measures, oversight policies on the use and operation of the system, and life-cycle costs and expenditure plans. In addition, to assess TSA's coordination with government stakeholders, we interviewed officials from the Terrorist Screening Center, U.S. Customs and Border Protection, and TSA's Office of Aviation Operations regarding coordination with TSA, and memorandums of understanding regarding services to be provided for Secure Flight during its testing phases and when fully operational. To assess TSA's external coordination, we interviewed officials from 4 large air carriers and 3 major privacy groups to discuss TSA's outreach efforts to the airline industry and to provide industry stakeholders with an opportunity to communicate perspectives about Secure Flight. We selected these air carriers and privacy groups due to their ongoing involvement with TSA during the CAPPS II project and the Secure Flight project. In addition, we had formal interviews with officials from two air carrier associations and these officials agreed subsequently to disseminate written questions regarding Secure Flight to their member air carriers. Officials from 14 air carriers emailed written responses to our questions regarding the development and implementation of Secure Flight. These 14 air carriers and their regional affiliates accounted for 91 percent of all domestic enplanements during the 1-year period from October 2003 until September 2004. Because we selected non-probability samples of air carriers and privacy groups, the results of the interviews with air carrier and privacy group officials and the written responses provided by air carrier officials cannot be generalized to the airline industry or all privacy groups. In assessing TSA's efforts to provide program oversight and management and to coordinate with stakeholders, we addressed the specific mandated issues identified in Public Law 108-334 related to (1) the establishment of an internal oversight board to monitor the manner in which Secure Flight is being developed; (2) the incorporation of operational safeguards to reduce opportunities for abuse; (3) the establishment of security measures to protect Secure Flight from unauthorized users; (4) the adoption of policies establishing effective oversight of the use and operation of the system; and (5) the existence of appropriate life-cycle cost estimates and expenditure and program plans.

To examine the efforts being taken to minimize the impacts of Secure Flight on passengers and protect passenger rights, we assessed TSA's efforts to address Privacy Act requirements[2] and Fair Information Practices,[3] as well as TSA's plans for developing a system of redress for passengers identified for additional screening or denied boarding based on Secure Flight. We analyzed TSA's documentation on privacy issues, such as the draft redress process, and interviewed agency officials with privacy-related responsibilities, including TSA's Privacy Officer. We also reviewed data on TSA's current redress process. We also interviewed officials from several privacy advocacy organizations to gain insight into privacy concerns regarding Secure Flight. In addition, we assessed TSA's efforts to address international privacy concerns regarding Secure Flight, which were a key concern during the development of CAPPS II. In determining the efforts being taken to minimize the impacts on passengers and protect passenger rights, we addressed the specific mandated issues identified in Public Law 108-334 related to (1) the assurance that there are no specific privacy concerns with the technological architecture of the system, and (2) TSA having a system in place whereby passengers determined to pose a threat may appeal such decision and correct erroneous information contained in Secure Flight.

As described above, in answering these four questions, we addressed the 10 specific issues we were mandated to review by Public Law 108-334.[4] Table 4 describes the 10 issues and provides a cross-reference to the sections in this report that address each issue. TSA has not made key decisions concerning Secure Flight's implementation and operations and, therefore, documents describing many of these issues, such as final security plans, privacy impact assessments, and a redress process, have not been developed or finalized. As a result, since Secure Flight is currently undergoing development and testing, and the system is not yet operational, we assessed the 10 areas we were mandated to review based

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

[3] 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.

[4] The Department of Homeland Security Appropriations Act, 2005, mandated that the GAO report to the Committees on Appropriations of the Senate and the House of Representatives on ten issues related to the development and implementation of Secure Flight, including system development and security, privacy, redress, oversight and other issues listed in table 4.

on the current stage of the system's development. We conducted our work from April 2004 until March 2005 in accordance with generally accepted government auditing standards.

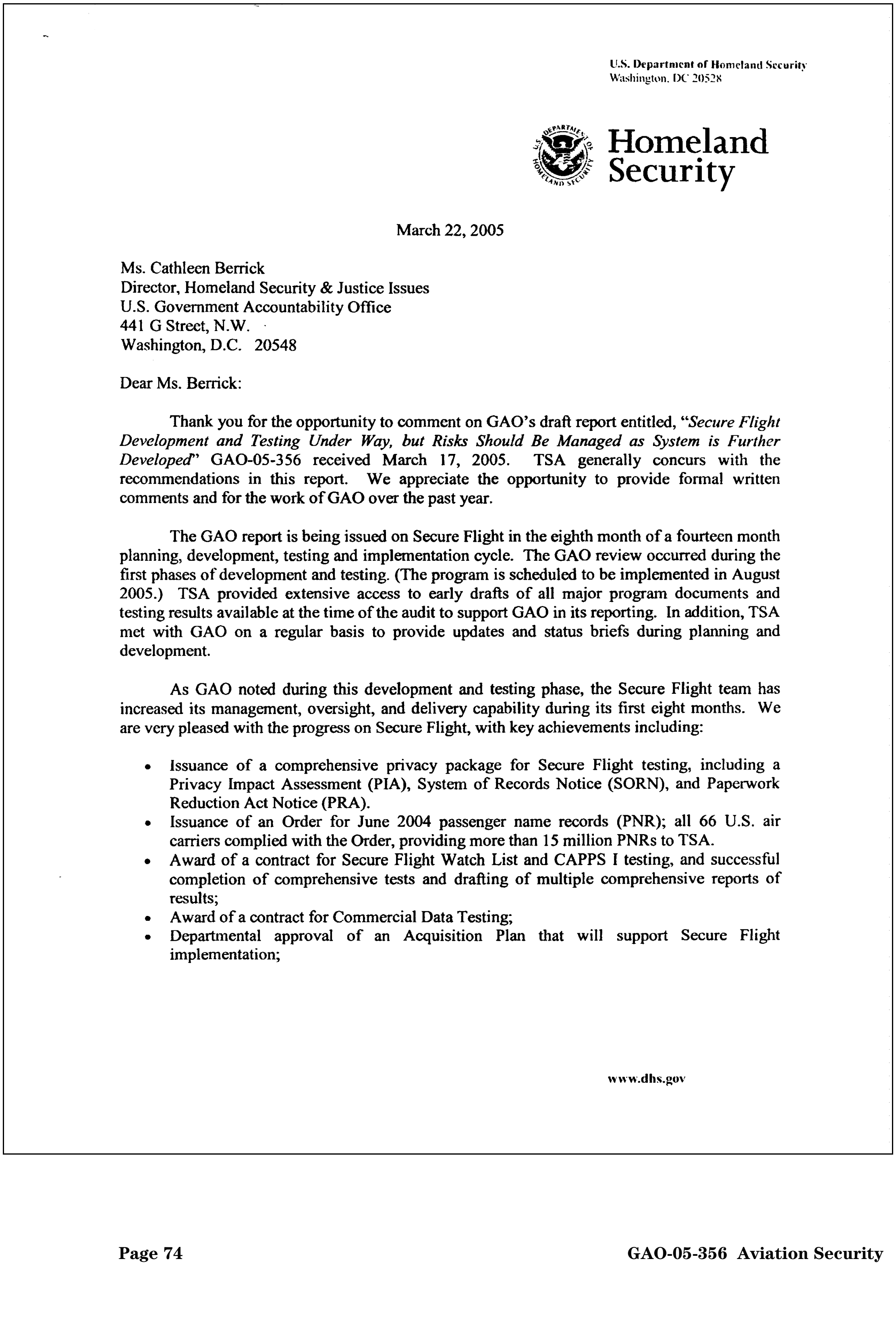
Table 5: Cross-references of Legislatively Mandated Issues to Be Reviewed by GAO with the Sections in this Report

		Report sections/questions			
Legislative mandated issue (number and short title)	**Description of mandated issue**	**1. Status of development and implementation**	**2. Factors affecting effectiveness**	**3. Processes for oversight and management**	**4. Privacy and redress**
1. Redress process	A system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights by the TSA may appeal such decisions and correct erroneous information contained in CAPPS II or Secure Flight or other follow-on/successor programs.				X
2. Accuracy of databases and effectiveness of Secure Flight	The underlying error rate of the government and private databases that will be used to both 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.		X		
3. Stress testing	TSA has stress-tested and demonstrated the efficacy and accuracy of all search tools in CAPPS II or Secure Flight or other follow-on/successor programs and has demonstrated that CAPPS II or Secure Flight or other follow-on/successor programs can make an accurate predictive assessment of those passengers who may constitute a threat to aviation.	X			

Legislative mandated issue (number and short title)	Description of mandated issue	Report sections/questions 1. Status of development and implementation	2. Factors affecting effectiveness	3. Processes for oversight and management	4. Privacy and redress
4. Internal oversight	The Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II or Secure Flight or other follow-on/successor programs are being developed and prepared.			X	
5. Operational safeguards	TSA has built in sufficient operational safeguards to reduce the opportunities for abuse.			X	
6. Security measures	Substantial security measures are in place to protect CAPPS II or Secure Flight or other follow-on/successor programs from unauthorized access by hackers or other intruders.			X	
7. Oversight of system use and operation	TSA has adopted policies establishing effective oversight of the use and operation of the system.			X	
8. Privacy concerns	There are no specific privacy concerns with the technological architecture of the system.				X
9. Modifications with respect to intrastate travel to accommodate states with unique air transportation needs	TSA has, in accordance with the requirements of section 44903 (j)(2)(B) of title 49, United States Code, modified CAPPS II or Secure Flight or other follow-on/successor programs with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger primary selectee status.		X		
10. Life-cycle cost estimates and expenditure plans	Appropriate life-cycle cost estimates, and expenditure and program plans exist.			X	

Source: GAO.

Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

March 22, 2005

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

Dear Ms. Berrick:

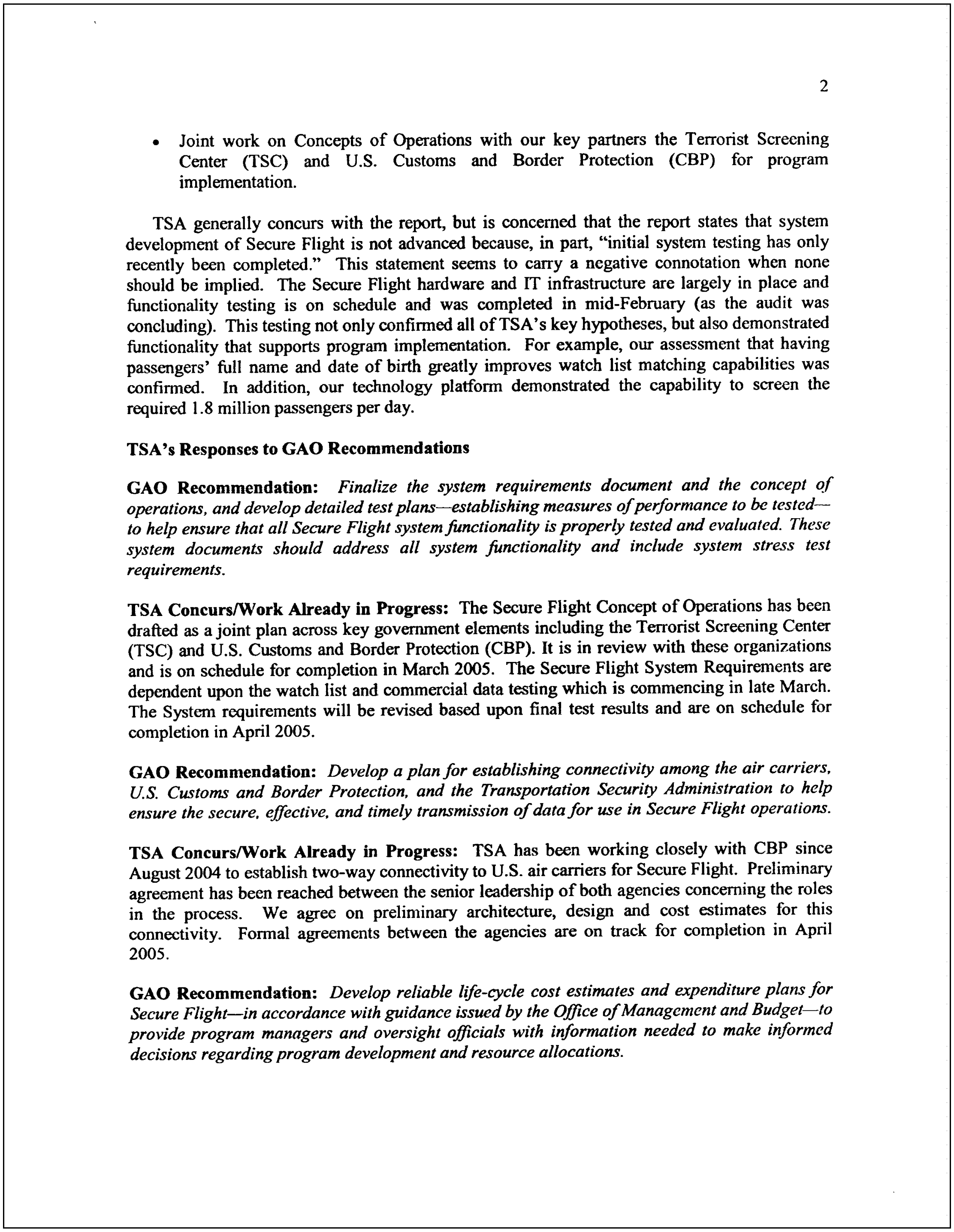
Thank you for the opportunity to comment on GAO's draft report entitled, "*Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed*" GAO-05-356 received March 17, 2005. TSA generally concurs with the recommendations in this report. We appreciate the opportunity to provide formal written comments and for the work of GAO over the past year.

The GAO report is being issued on Secure Flight in the eighth month of a fourteen month planning, development, testing and implementation cycle. The GAO review occurred during the first phases of development and testing. (The program is scheduled to be implemented in August 2005.) TSA provided extensive access to early drafts of all major program documents and testing results available at the time of the audit to support GAO in its reporting. In addition, TSA met with GAO on a regular basis to provide updates and status briefs during planning and development.

As GAO noted during this development and testing phase, the Secure Flight team has increased its management, oversight, and delivery capability during its first eight months. We are very pleased with the progress on Secure Flight, with key achievements including:

- Issuance of a comprehensive privacy package for Secure Flight testing, including a Privacy Impact Assessment (PIA), System of Records Notice (SORN), and Paperwork Reduction Act Notice (PRA).
- Issuance of an Order for June 2004 passenger name records (PNR); all 66 U.S. air carriers complied with the Order, providing more than 15 million PNRs to TSA.
- Award of a contract for Secure Flight Watch List and CAPPS I testing, and successful completion of comprehensive tests and drafting of multiple comprehensive reports of results;
- Award of a contract for Commercial Data Testing;
- Departmental approval of an Acquisition Plan that will support Secure Flight implementation;

www.dhs.gov



- Joint work on Concepts of Operations with our key partners the Terrorist Screening Center (TSC) and U.S. Customs and Border Protection (CBP) for program implementation.

TSA generally concurs with the report, but is concerned that the report states that system development of Secure Flight is not advanced because, in part, "initial system testing has only recently been completed." This statement seems to carry a negative connotation when none should be implied. The Secure Flight hardware and IT infrastructure are largely in place and functionality testing is on schedule and was completed in mid-February (as the audit was concluding). This testing not only confirmed all of TSA's key hypotheses, but also demonstrated functionality that supports program implementation. For example, our assessment that having passengers' full name and date of birth greatly improves watch list matching capabilities was confirmed. In addition, our technology platform demonstrated the capability to screen the required 1.8 million passengers per day.

TSA's Responses to GAO Recommendations

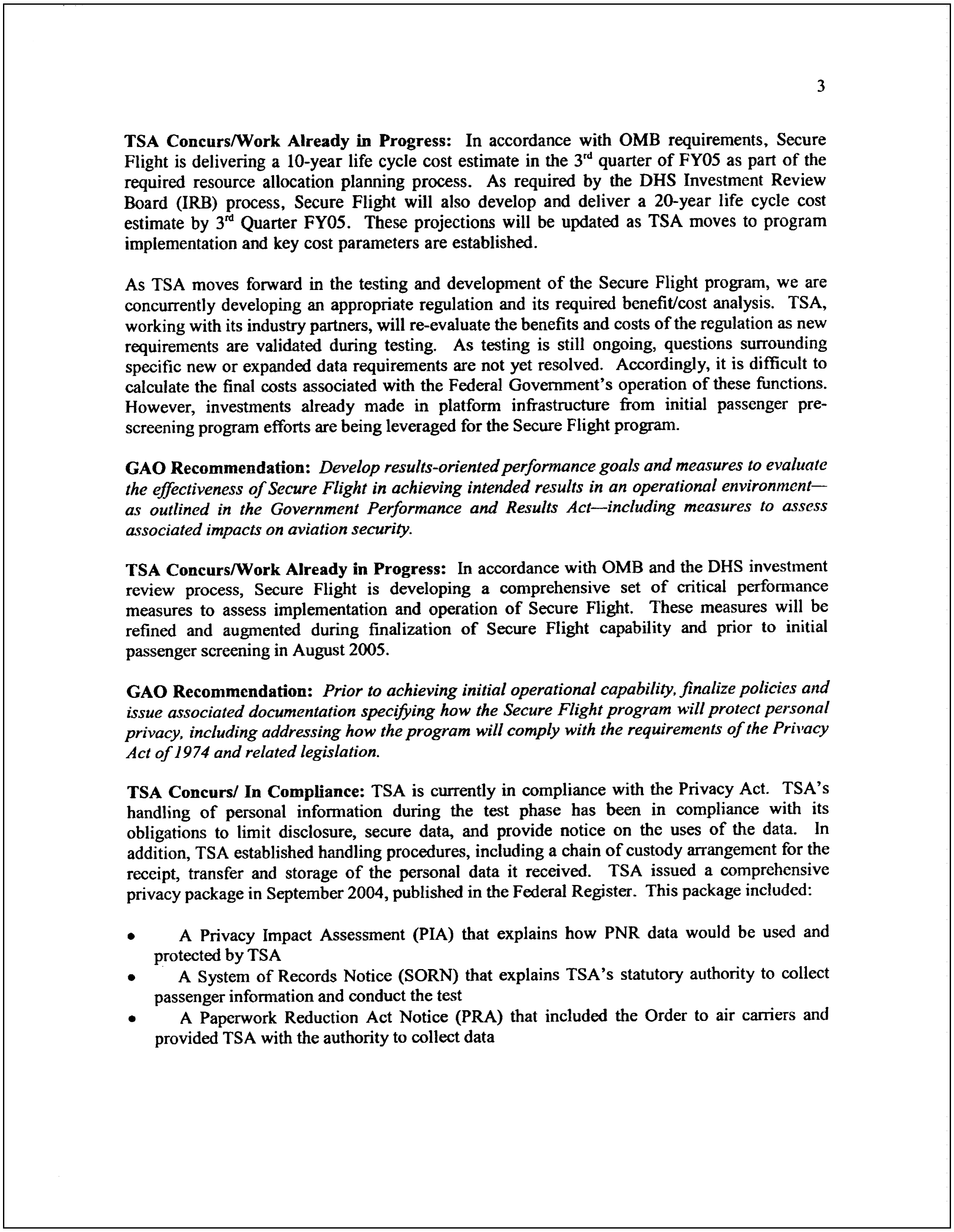
GAO Recommendation: *Finalize the system requirements document and the concept of operations, and develop detailed test plans—establishing measures of performance to be tested—to help ensure that all Secure Flight system functionality is properly tested and evaluated. These system documents should address all system functionality and include system stress test requirements.*

TSA Concurs/Work Already in Progress: The Secure Flight Concept of Operations has been drafted as a joint plan across key government elements including the Terrorist Screening Center (TSC) and U.S. Customs and Border Protection (CBP). It is in review with these organizations and is on schedule for completion in March 2005. The Secure Flight System Requirements are dependent upon the watch list and commercial data testing which is commencing in late March. The System requirements will be revised based upon final test results and are on schedule for completion in April 2005.

GAO Recommendation: *Develop a plan for establishing connectivity among the air carriers, U.S. Customs and Border Protection, and the Transportation Security Administration to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations.*

TSA Concurs/Work Already in Progress: TSA has been working closely with CBP since August 2004 to establish two-way connectivity to U.S. air carriers for Secure Flight. Preliminary agreement has been reached between the senior leadership of both agencies concerning the roles in the process. We agree on preliminary architecture, design and cost estimates for this connectivity. Formal agreements between the agencies are on track for completion in April 2005.

GAO Recommendation: *Develop reliable life-cycle cost estimates and expenditure plans for Secure Flight—in accordance with guidance issued by the Office of Management and Budget—to provide program managers and oversight officials with information needed to make informed decisions regarding program development and resource allocations.*



TSA Concurs/Work Already in Progress: In accordance with OMB requirements, Secure Flight is delivering a 10-year life cycle cost estimate in the 3rd quarter of FY05 as part of the required resource allocation planning process. As required by the DHS Investment Review Board (IRB) process, Secure Flight will also develop and deliver a 20-year life cycle cost estimate by 3rd Quarter FY05. These projections will be updated as TSA moves to program implementation and key cost parameters are established.

As TSA moves forward in the testing and development of the Secure Flight program, we are concurrently developing an appropriate regulation and its required benefit/cost analysis. TSA, working with its industry partners, will re-evaluate the benefits and costs of the regulation as new requirements are validated during testing. As testing is still ongoing, questions surrounding specific new or expanded data requirements are not yet resolved. Accordingly, it is difficult to calculate the final costs associated with the Federal Government's operation of these functions. However, investments already made in platform infrastructure from initial passenger pre-screening program efforts are being leveraged for the Secure Flight program.

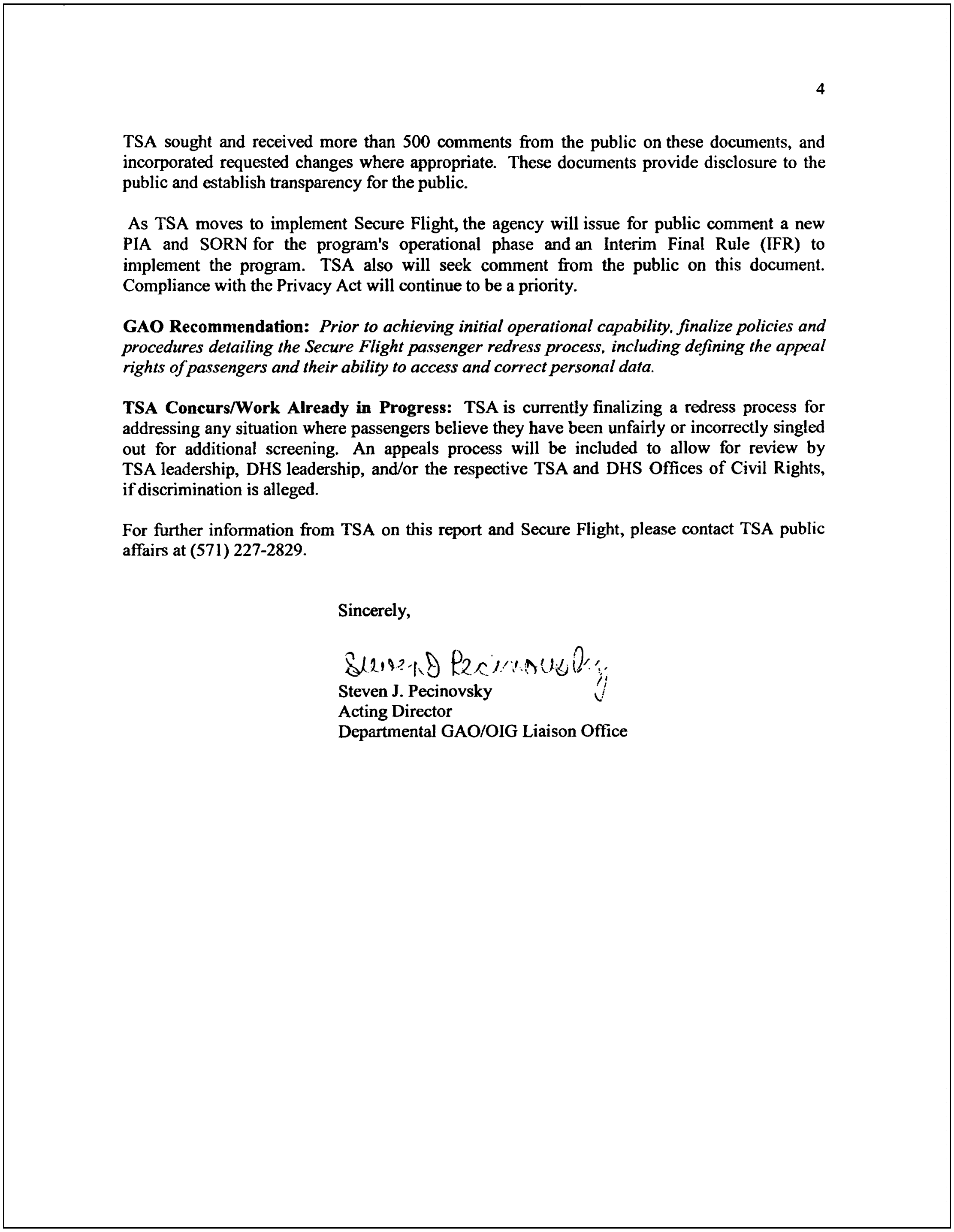
GAO Recommendation: *Develop results-oriented performance goals and measures to evaluate the effectiveness of Secure Flight in achieving intended results in an operational environment—as outlined in the Government Performance and Results Act—including measures to assess associated impacts on aviation security.*

TSA Concurs/Work Already in Progress: In accordance with OMB and the DHS investment review process, Secure Flight is developing a comprehensive set of critical performance measures to assess implementation and operation of Secure Flight. These measures will be refined and augmented during finalization of Secure Flight capability and prior to initial passenger screening in August 2005.

GAO Recommendation: *Prior to achieving initial operational capability, finalize policies and issue associated documentation specifying how the Secure Flight program will protect personal privacy, including addressing how the program will comply with the requirements of the Privacy Act of 1974 and related legislation.*

TSA Concurs/ In Compliance: TSA is currently in compliance with the Privacy Act. TSA's handling of personal information during the test phase has been in compliance with its obligations to limit disclosure, secure data, and provide notice on the uses of the data. In addition, TSA established handling procedures, including a chain of custody arrangement for the receipt, transfer and storage of the personal data it received. TSA issued a comprehensive privacy package in September 2004, published in the Federal Register. This package included:

- A Privacy Impact Assessment (PIA) that explains how PNR data would be used and protected by TSA
- A System of Records Notice (SORN) that explains TSA's statutory authority to collect passenger information and conduct the test
- A Paperwork Reduction Act Notice (PRA) that included the Order to air carriers and provided TSA with the authority to collect data



TSA sought and received more than 500 comments from the public on these documents, and incorporated requested changes where appropriate. These documents provide disclosure to the public and establish transparency for the public.

As TSA moves to implement Secure Flight, the agency will issue for public comment a new PIA and SORN for the program's operational phase and an Interim Final Rule (IFR) to implement the program. TSA also will seek comment from the public on this document. Compliance with the Privacy Act will continue to be a priority.

GAO Recommendation: *Prior to achieving initial operational capability, finalize policies and procedures detailing the Secure Flight passenger redress process, including defining the appeal rights of passengers and their ability to access and correct personal data.*

TSA Concurs/Work Already in Progress: TSA is currently finalizing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening. An appeals process will be included to allow for review by TSA leadership, DHS leadership, and/or the respective TSA and DHS Offices of Civil Rights, if discrimination is alleged.

For further information from TSA on this report and Secure Flight, please contact TSA public affairs at (571) 227-2829.

Sincerely,

Steven J. Pecinovsky
Acting Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen A. Berrick (202) 512-3404
David A. Powner (202) 512-9286
Christine Fossett (202) 512-2956

Staff Acknowledgments

In addition to the above, J. Michael Bollinger, Grace Coleman, John de Ferrari, R. Denton Herring, Adam Hoffman, David Hooper, Linda Koontz, Thomas Lombardi, Michele Mackin, Colleen Phillips, Jamie Pressman, David Plocher, John R. Schulze, Karl Seifert, Adam Vodraska, and Eric Winter made key contributions to this report.

GAO Related Products

Aviation Security: Systematic Planning Needed to Optimize the Development of Checked Baggage Screening Systems. GAO-05-365. Washington, D.C.: March 15, 2005.

Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program. GAO-05-324. Washington, D.C.: February 23, 2005.

Transportation Security: Systematic Planning Needed to Optimize Resources. GAO-05-357T. Washington, D.C.: February 15, 2005.

Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach. GAO-04-702. Washington, D.C.: August 27, 2004.

Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts. GAO-04-592T. Washington, D.C.: March 30, 2004.

*Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System.*GAO-04-504T. Washington, D.C.: March 17, 2004.

Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385. Washington, D.C.: February 13, 2004.

Information Technology: OMB and Department of Homeland Security Investment Reviews. GAO-04-323. Washington, D.C.: February 10, 2004.

Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs. GAO-04-285T. Washington, D.C.: November 20, 2003.

Aviation Security: Efforts to Measure Effectiveness and Address Challenges. GAO-04-232T. Washington, D.C.: November 5, 2003.

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

Transportation Security: Federal Action Needed to Enhance Security Efforts. GAO-03-1154T. Washington, D.C.: September 9, 2003. , September 9, 2003.

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

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

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER