United States Government Accountability Office

GAO

Testimony before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, June 14, 2006

# AVIATION SECURITY

# Management Challenges Remain for the Transportation Security Administration's Secure Flight Program

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

Accountability ★ Integrity ★ Reliability

GAO

Accountability·Integrity·Reliability

# Highlights

Highlights of GAO-06-864T, a testimony before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives

## Why GAO Did This Study

After the events of September 11, 2001, the Transportation Security Administration (TSA) assumed the function of passenger prescreening—or the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny—for domestic flights, which is currently performed by the air carriers. To do so, TSA has been developing Secure Flight. This testimony covers TSA's progress and challenges in (1) developing, managing, and overseeing Secure Flight; (2) coordinating with key stakeholders critical to program operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing impacts on passenger privacy and protecting passenger rights.

## What GAO Recommends

A prior GAO report recommended that the Department of Homeland Security (DHS) direct TSA to take several actions to manage risks associated with Secure Flight's development, including finalizing system requirements, test plans, privacy and redress requirements, and program cost estimates, and establishing plans to obtain data needed to operate the system. DHS generally concurred with GAO's recommendations, but has not yet completed the actions it planned to take. TSA's rebaselining effort is reassessing program goals, requirements, and capabilities.

www.gao.gov/cgi-bin/getrpt?GAO-06-864T.

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

June 14, 2006

# AVIATION SECURITY

# Management Challenges Remain for the Transportation Security Administration's Secure Flight Program

## What GAO Found

For over 3 years, TSA has faced challenges in developing and implementing the Secure Flight program, and in early 2006, it suspended Secure Flight's development to reassess, or rebaseline, the program. TSA's rebaselining effort is currently under way, and final decisions regarding the future direction of the program have not been made. In our most recent report and testimony, we noted that TSA had made some progress in developing and testing the Secure Flight program, but had not followed a disciplined life cycle approach to manage systems development or fully defined system requirements. We also reported that TSA was proceeding to develop Secure Flight without a program management plan containing program schedule and cost estimates. Oversight reviews of the program had also raised questions about program management. Secure Flight officials stated that as they move forward with the rebaselined program, they will be following a more rigorous and disciplined life cycle process for Secure Flight. We support TSA's rebaselining effort, and believe that the agency should not move forward with the program until it has demonstrated that a disciplined life cycle process is being followed.

We also reported that TSA had taken steps to collaborate with Secure Flight stakeholders whose participation is essential to ensuring that passenger and terrorist watch list data are collected and transmitted to support Secure Flight. However, key program stakeholders—including the U.S. Customs and Border Protection, the Terrorist Screening Center, and air carriers—stated that they needed more definitive information about system requirements from TSA to plan for their support of the program.

In addition, we reported that several activities that will affect Secure Flight's effectiveness were under way or had not yet been decided. For example, TSA conducted name-matching tests that compared passenger and terrorist screening database information to determine what type of passenger data would be needed for Secure Flight's purposes. However, TSA had not yet made key policy decisions that could significantly impact program operations, including what passenger data it would require air carriers to provide and the name-matching technologies it would use.

Further, Secure Flight's system development documentation did not fully identify how passenger privacy protections were to be met, and TSA had not issued the privacy notices that described how it would protect passenger data once Secure Flight became operational. As a result, it was not possible to assess how TSA is addressing privacy concerns. Secure Flight officials stated that they plan to address privacy issues and finalize its redress polices in conjunction with rebaselining the program.

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the Transportation Security Administration's (TSA) intelligence efforts and the integration of its programs that will affect the traveling public, such as Secure Flight. The purpose of Secure Flight is to enable our government to protect the public and strengthen aviation security by identifying and scrutinizing individuals suspected of having ties to terrorism, or who may otherwise pose a threat to aviation, in order to prevent them from boarding commercial aircraft in the United States, if warranted, or by subjecting them to additional security scrutiny prior to boarding an aircraft. The program also aims to reduce the number of individuals unnecessarily selected for secondary screening while protecting passengers' privacy and civil liberties.

My testimony today summarizes the progress TSA has made to develop and implement Secure Flight and the challenges it continues to face as it moves forward with (1) developing, managing, and overseeing the Secure Flight program; (2) coordinating with federal and private sector stakeholders who will play critical roles in Secure Flight operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing program impacts on passenger privacy and protecting passenger rights. Since I last testified on these issues in February 2006,[1] TSA announced that it was rebaselining the Secure Flight program. This rebaselining effort includes reassessing program goals to be achieved, expected benefits and capabilities, and estimated schedules and costs.

My testimony is based on our March 2005 report,[2] other past reviews of the Secure Flight program (see app. I for a list of GAO products issued on Secure Flight), and preliminary results from our ongoing review of 10 issues related to the development and implementation of Secure Flight, as mandated by Public Law 109-90, and as requested by eight

[1] GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program,* GAO-06-374T (Washington, D.C.: Feb. 9, 2006).

[2] GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,* GAO-05-356 (Washington, D.C.: March 2005).

congressional committees.[3] (See app. II for a description of the 10 issues and app. III for additional information on the scope and methodology for this review.) In March 2005, we reported that TSA had made progress in developing and testing Secure Flight, but had not completed key system testing, had not finalized system requirements or determined how certain aspects of the program would operate (such as the basis on which passengers would be selected for preflight scrutiny), and had not clearly defined the privacy impacts of the program. At the time, we recommended that TSA take several actions to manage the risks associated with developing and implementing Secure Flight, including finalizing system requirements and test plans, privacy and redress requirements, and program cost estimates. In February 2006, we testified that TSA had committed to take action based on our recommendations that the agency manage the risks associated with developing and implementing Secure Flight. Although we noted that TSA had made some progress in these areas, we reported that it had not completed any of the actions that were scheduled to be accomplished and long-standing issues related to systems development and testing, program management, and privacy and redress protections remained. Following our February 2006 testimony, TSA announced a temporary suspension of Secure Flight's development to rebaseline the program.

## Summary

For over 3 years, TSA has faced significant challenges in developing and implementing the Secure Flight program, a federal passenger prescreening initiative. As we testified in February 2006:

- TSA had not conducted critical development activities, such as following a disciplined life cycle approach for all phases of development, in

[3] Section 518 of the Department of Homeland Security Appropriations Act, 2006 (Pub. L. No. 109-90) requires GAO to report to the Committees on Appropriations of the Senate and House of Representatives on the 10 issues listed in § 522(a) the Department of Homeland Security Appropriations Act, 2005 (Pub. L. No. 108-334), not later than 90 days after the Secretary of the Department of Homeland Security certifies to the above-named committees that Secure Flight has satisfied the 10 issues. These 10 issues relate to system development and implementation, effectiveness, program management and oversight, and privacy and redress. We are also conducting our ongoing review in response to requests from the United States Senate: the Committee on Commerce, Science, and Transportation, and its Subcommittee on Aviation; Committee on Appropriations, Subcommittee on Homeland Security; Committee on Homeland Security and Governmental Affairs; Committee on Judiciary; also the House of Representatives: Committee on Transportation and Infrastructure, Committee on Homeland Security; and the Chairman of the Committee on Government Reform.

accordance with best practices for large-scale information technology programs, potentially putting the program at risk of failure. In addition, TSA had not maintained up-to-date program schedules or developed cost estimates for the program.

- TSA had made progress in coordinating with stakeholders—U.S. Customs and Border Protection (CBP), Terrorist Screening Center (TSC), and air carriers—but additional information and testing were needed before stakeholders could be in a position to provide the support required for Secure Flight to function as intended.

- TSA made some progress in evaluating factors that could influence Secure Flight's effectiveness. However, key policy decisions—such as what data TSA will require air carriers to collect to support Secure Flight operations—and related efforts, to include operational testing, had not been completed.

- Secure Flight's system documentation had not fully addressed how passenger privacy protections were to be met, and therefore potential impacts on privacy could not be assessed. Such an assessment will not be possible until TSA determines, among other things, what passenger data it will require for Secure Flight operations. We further reported that TSA had not yet determined how it would include a process of appeals for travelers erroneously singled out as part of the prescreening process.

TSA has acknowledged these challenges and, based in part on our prior recommendations, has been taking corrective actions. In early 2006, TSA suspended development of Secure Flight and initiated a reassessment, or rebaselining, of the program, to be completed before moving forward. This rebaselining effort is currently under way, and decisions regarding the future direction of the program have not been made. We support TSA's rebaselining effort, and believe that the agency should not move forward with the program until it demonstrates that it is following a disciplined life cycle process.

## Background

TSA is responsible for securing all modes of transportation while facilitating commerce and the freedom of movement for the traveling public. Passenger prescreening is one program among many that TSA uses to secure the domestic aviation sector. The process of prescreening passengers—that is, determining whether airline passengers might pose a security risk before they reach the passenger-screening checkpoint—is used to focus security efforts on those passengers that represent the greatest potential threat. Currently, U.S. air carriers conduct passenger prescreening by comparing passenger names against government-supplied terrorist watch lists and applying the Computer-Assisted Passenger Prescreening System rules, known as CAPPS rules.[4]

## Development of Legacy Passenger Prescreening Systems

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,[5] 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[6] over the current prescreening process, and to screen all passengers flying into, out of, and within the United States.

Based in part on concerns about privacy and other issues expressed by us and others, the Department of Homeland Security (DHS) canceled the development of CAPPS II in August 2004. Shortly thereafter, it announced that it planned to develop a new passenger prescreening program called Secure Flight. In contrast to CAPPS II, Secure Flight, among other changes, will only prescreen passengers flying domestically within the United States, rather than passengers flying into and out of the United States. Also, the CAPPS rules will not be implemented as part of Secure Flight, but rather the rules will continue to be applied by commercial air carriers. As of February 2006, TSA planned to operate Secure Flight on the

[4] CAPPS rules are characteristics that are used to select passengers who require additional security scrutiny. CAPPS rules are Sensitive Security Information.

[5] Aviation and Transportation Security Act, Pub. L. No. 107-71, § 136, 115 Stat. 597, 637 (2001).

[6] The second generation passenger screening system anticipated improvements in security by moving the watch list screening process within the federal government so that comparisons could be made using a single system, rather than the multiple matching programs now utilized by individual air carriers. Further, security would be enhanced by vetting passengers against the expanded watch lists produced by TSC, instead of the more limited lists currently transmitted to air carriers.

Transportation Vetting Platform (TVP)[7]—the underlying infrastructure (hardware and software) developed to support the Secure Flight application, including security, communications, and data management and, the Secure Flight application was to perform the functions associated with receiving, vetting, and returning requests related to the determination of whether passengers are on government watch lists. This application was also to be configurable—meaning that it could be quickly adjusted to reflect changes to workflow parameters. In May 2006, TSA officials stated that the agency was considering other approaches for integrating the Secure Flight TVP and application functions in a different configuration as part of rebaselining the program. In its rebaselining effort, this and other aspects of Secure Flight are currently being reviewed, and policy decisions regarding the operations of the program have not been finalized.[8]

## Overview of TSA's Plans to Operate Secure Flight as of February 2006

As envisioned under Secure Flight, when a passenger made flight arrangements, the organization accepting the reservation, such as the air carrier's reservation office or a travel agent, would enter passenger name record (PNR) information obtained from the passenger, which would then be stored in the air carrier's reservation system.[9] While the government would be asking for only portions of the PNR, the PNR data could include the passenger's name, phone number, number of bags, seat number, and form of payment, among other information. Approximately 72 hours prior to the flight, portions of the passenger data contained in the PNR would be sent to Secure Flight through a secure network connection provided by

[7] TSA planned to use this centralized vetting capability to identify terrorist threats in support of various DHS and TSA programs. In addition to Secure Flight, TSA planned 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 expected 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.

[8] The Intelligence Reform and Terrorism Prevention Act of 2004 requires that TSA begin to assume responsibility for the passenger prescreening function within 180 days after the completion of testing. Pub. L. No. 108-458 § 4012, 118 Stat. 3638, 3714-19 (codified as amended at 49 U.S.C. § 44903(j)(2)).

[9] This description of the Secure Flight system, as well as the graphic illustrating the system in figure1, is based on TSA's draft June 9, 2005, concept of operations, a document that gives a high-level overview of the Secure Flight system.

DHS's CBP. Reservations or changes to reservations that were made less than 72 hours prior to flight time would be sent immediately to TSA through CBP.

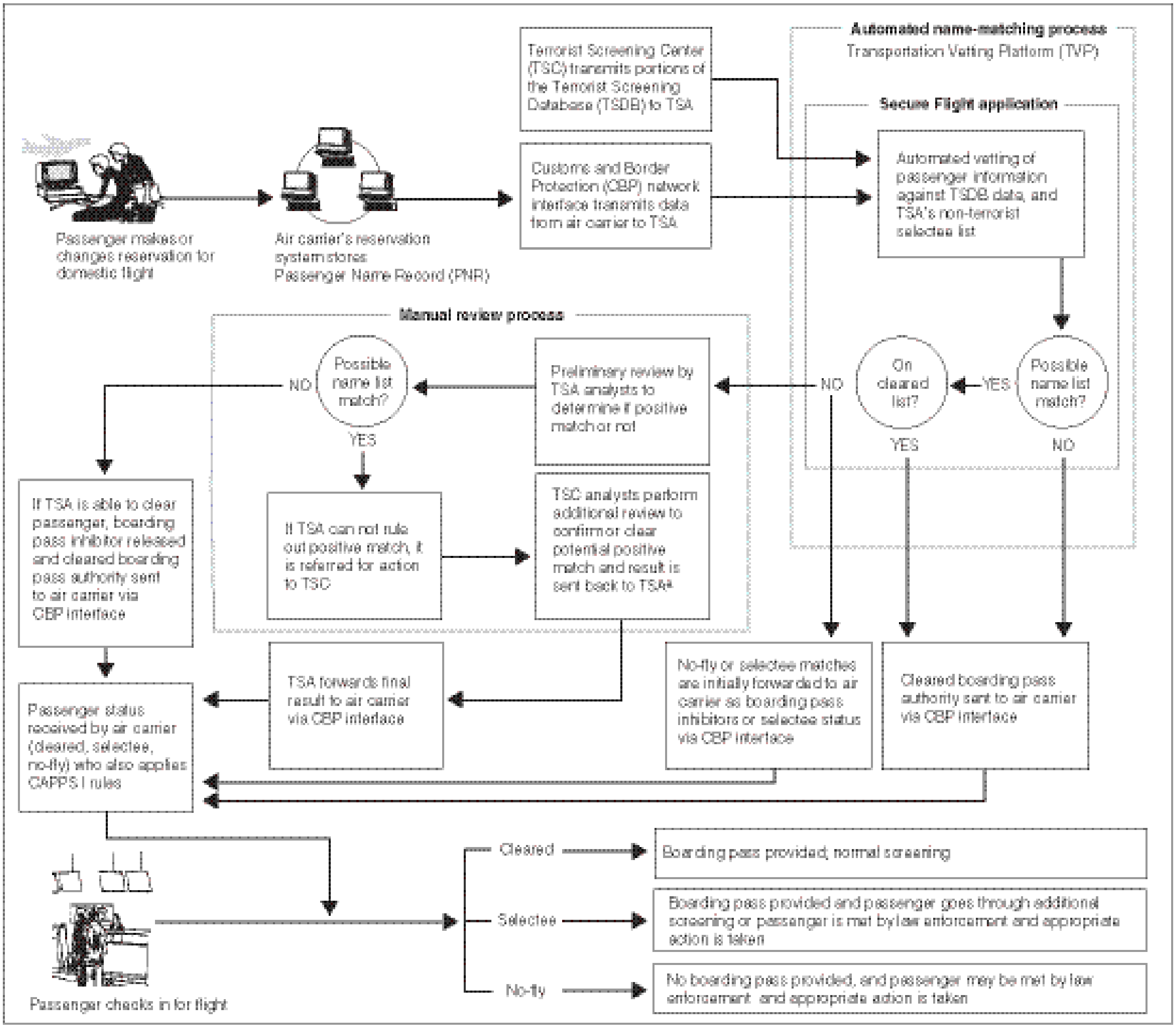
Upon receipt of passenger data, TSA planned to process the passenger data through the Secure Flight application running on the TVP. During this process, Secure Flight would determine if the passenger data matched the data extracted daily from TSC's Terrorist Screening Database (TSDB)—the information consolidated by TSC from terrorist watch lists to provide government screeners with a unified set of terrorist-related information. In addition, TSA would screen against its own watch list composed of individuals who do not have a nexus to terrorism but who may pose a threat to aviation security.[10]

In order to match passenger data to information contained in the TSDB, TSC planned to provide TSA with an extract of the TSDB for use in Secure Flight and provide updates as they occur. This TSDB subset would include all individuals classified as either selectees (individuals who are selected for additional security measures prior to boarding an aircraft) or no-flys (individuals who would be denied boarding unless they are cleared by law enforcement personnel).[11] To perform the match, Secure Flight was to compare the passenger data, TSDB, and other watch list data using automated name-matching technologies. When a possible match was generated, TSA and potentially TSC analysts would conduct a manual review comparing additional law enforcement and other government information with passenger data to determine if the person could be ruled out as a possible match. TSA was to return the matching results to the air carriers through CBP. Figure 1 illustrates how Secure Flight was intended to operate as of February 2006.

[10] TSA also planned to utilize a cleared list as part of the watch list matching process; the cleared list was to be composed of individuals who are frequently misidentified as being on the TSDB and who have applied, and been approved, to be on the list.

[11] These measures may include additional screening or other law enforcement actions.

Figure 1: Planned Operation of Secure Flight as of February 2006


Automated name-matching process
Transportation Vetting Platform (TVP)
Secure Flight application
Terrorist Screening Center (TSC) transmits portions of the Terrorist Screening Database (TSDB) to TSA
Customs and Border Protection (CBP) network interface transmits data from air carrier to TSA
Automated vetting of passenger information against TSDB data, and TSA's non-terrorist selectee list
Passenger makes or changes reservation for domestic flight
Air carrier's reservation system stores Passenger Name Record (PNR)
Manual review process
Possible name list match?
NO
YES
Preliminary review by TSA analysts to determine if positive match or not
NO
On cleared list?
YES
Possible name list match?
YES
NO
If TSA is able to clear passenger, boarding pass inhibitor released and cleared boarding pass authority sent to air carrier via CBP interface
If TSA can not rule out positive match, it is referred for action to TSC
TSC analysts perform additional review to confirm or clear potential positive match and result is sent back to TSA[a]
Passenger status received by air carrier (cleared, selectee, no-fly) who also applies CAPPS I rules
TSA forwards final result to air carrier via CBP interface
No-fly or selectee matches are initially forwarded to air carrier as boarding pass inhibitors or selectee status via CBP interface
Cleared boarding pass authority sent to air carrier via CBP interface
Cleared
Boarding pass provided; normal screening
Selectee
Boarding pass provided and passenger goes through additional screening or passenger is met by law enforcement and appropriate action is taken
No-fly
No boarding pass provided, and passenger may be met by law enforcement and appropriate action is taken
Passenger checks in for flight

Source: GAO analysis of TSA data.

[a]Information about confirmed no-flys and certain selectees are shared with appropriate federal agencies which coordinate the appropriate law enforcement response.

As shown in figure 1, when the passenger checked in for the flight at the airport, the passenger was to receive a level of screening based on his or her designated category. A cleared passenger was to be provided a boarding pass and allowed to proceed to the screening checkpoint in the normal manner. A selectee passenger was to receive additional security scrutiny at the screening checkpoint.[12] A no-fly passenger would not be issued a boarding pass. Instead, appropriate law enforcement agencies would be notified. Law enforcement officials would determine whether the individual would 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. Based on its rebaselining effort, TSA may modify this concept of operations for Secure Flight.

## TSA Had Not Followed a Disciplined Life Cycle Approach or Fully Defined System Requirements, Schedule, and Costs

As we testified in February 2006, TSA had not conducted critical activities in accordance with best practices for large-scale information technology programs. Further, TSA had not followed a disciplined life cycle approach in developing Secure Flight, in which all phases of the project are defined by a series of orderly phases and the development of related documentation. Program officials stated that they had instead used a rapid development method that was intended to enable them to develop the program more quickly. However, as a result of this approach, the development process had been ad hoc, with project activities conducted out of sequence. For example, program officials declared the design phase complete before requirements for designing Secure Flight had been detailed.

Our evaluations of major federal information technology programs, and research by others, have shown that following a disciplined life cycle management process decreases the risks associated with acquiring systems. As part of the life cycle process, TSA must define and document Secure Flight's requirements—including how Secure Flight is to function and perform, the data needed for the system to function, how various

[12] Some selectees were to receive a boarding pass from air carriers, but be required to undergo secondary screening prior to boarding the aircraft, while other selectees were to first be met by law enforcement personnel, who would determine if the individual should receive a boarding pass. In addition, air carriers, through their application of the CAPPS rules, could also designate a passenger as a selectee.

systems interconnect, and how system security is achieved. We found that Secure Flight's requirements documentation contained contradictory and missing information. TSA officials acknowledged that they had not followed a disciplined life cycle approach in developing Secure Flight, but stated that in moving forward, they would follow TSA's standard development process. We also found that while TSA had taken steps to implement an information security management program for protecting Secure Flight information and assets, its efforts were incomplete, based on federal standards and industry best practices. We reported that without a completed system security program, Secure Flight may not be adequately protected against unauthorized access and use or disruption, once the program becomes operational.

Further, TSA had proceeded with Secure Flight development without an effective program management plan that contained up-to-date program schedules and cost estimates. TSA officials stated they had not maintained an updated schedule in part because the agency had not promulgated a necessary regulation requiring commercial air carriers to submit certain passenger data needed to operate Secure Flight, and air carrier responses to this regulation would impact when Secure Flight would be operational and at what cost. While we recognized that program unknowns introduce uncertainty into the program-planning process, uncertainty is a practical reality in planning all programs and is not a reason for not developing plans, including cost and schedule estimates that reflect known and unknown aspects of the program.

Prior to TSA's rebaselining effort of Secure Flight, several oversight reviews of the program had been conducted that raised questions about program management, including the lack of fully defined requirements. DHS and TSA had executive and advisory oversight mechanisms in place to oversee Secure Flight, including the DHS Investment Review Board—designed to review certain programs at key phases of development to help ensure they met mission needs at expected levels of costs and risks. However, the DHS Investment Review Board and other oversight groups had identified problems with Secure Flight's development. Specifically, in January 2005, the Investment Review Board withheld approval of the TVP, which supported Secure Flight operations, to proceed from development and testing into production and deployment until a formal acquisition plan, a plan for integrating and coordinating Secure Flight with other DHS people-screening programs, and a revised acquisition program baseline had been completed. In addition, an independent working group within the Aviation Security Advisory Committee, composed of government, privacy, and security experts, reported in September 2005 that TSA had not produced a comprehensive policy document for Secure Flight that could define oversight or governance responsibilities, nor had it provided an accountability structure for the program.

TSA has taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, and suspended its development efforts while it rebaselines the program. This rebaselining effort includes reassessing program goals and capabilities and developing a new schedule and cost estimates. Although TSA officials stated that they will use a disciplined life cycle approach when moving forward with the rebaselined program, officials have not identified when their rebaselining effort will be completed.

## TSA Had Made Progress in Coordinating with Critical Stakeholders, but More Work Remains

As we testified in February 2006, TSA had taken steps to collaborate with Secure Flight stakeholders—CBP, TSC, and domestic air carriers—whose participation is essential to ensuring that passenger and terrorist watch list data are collected and transmitted for Secure Flight operations, but additional information and testing are needed to enable stakeholders to provide the necessary support for the program. TSA had, for example, drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and had begun receiving feedback from the air carriers on this information. TSA was also in the early stages of coordinating with CBP and TSC on broader issues of integration and interoperability related to other people-screening programs used by the government to combat terrorism.

Prior to its rebaselining effort, TSA had conducted preliminary network connectivity testing between TSA and federal stakeholders to determine, for example, how information would be transmitted from CBP to TSA and back. However, these tests used only dummy data and were conducted in a controlled environment, rather than in a real-world operational environment. According to CBP, without real data, it was not possible to conduct stress testing to determine if the system could handle the volume of data traffic that would be required by Secure Flight. TSA acknowledged it had not determined what the real data volume requirements would be, and could not do so until the regulation for air carriers was issued and their data management role had been finalized.

All key program stakeholders we interviewed stated that additional information was needed before they could finalize their plans to support Secure Flight operations. Although CBP, TSC, and air carrier officials we interviewed through January 2006 acknowledged TSA's outreach efforts, they cited several areas where additional information was needed from TSA before they could fully support Secure Flight. Several CBP officials stated, for example, that they could not proceed with establishing connectivity with all air carriers until DHS published the rule—the regulation that would specify what type of information was to be provided for Secure Flight—and the air carriers submitted their plans for providing this information. In addition, a TSC official stated that until TSA provided estimates of the volume of potential name matches that TSC would be required to screen, TSC could not make decisions about required resources.

TSA's ongoing coordination of prescreening and name-matching initiatives with CBP and TSC could impact how Secure Flight is implemented and require stakeholders to alter their plans made to support the program. In January 2006, TSA officials stated that they are coordinating more closely with CBP's international prescreening initiatives for passengers on flights bound for the United States. The Air Transport Association and the Association of European Airlines—organizations representing air carriers—had requested, among other things, that both domestic and international passenger prescreening function through coordinated information connections and avoid unnecessary duplication of communications, programming, and information requirements.[13] In addition, TSC has an initiative under way to, among other things, better safeguard watch list data. At present, TSC exports watch list data to other federal agencies for use in their screening efforts or processes for examining documents and records related to terrorism. However, TSC is currently developing a new system, Query, whereby watch list data would not be exported, but rather would be maintained by TSC. Query would serve as a common shared service that would allow agencies to directly search the TSDB using TSC's name-matching technology for their own purposes. If TSC chooses to implement Query, TSA may be required to modify the system architecture for Secure Flight in order to accommodate the new system.

Due to delays in Secure Flight's development and uncertainty about its future, officials from two air carriers told us after our February 2006 testimony that they were enhancing their respective name-matching systems because they were unsure when and whether TSA would be

[13] Correspondence to the Honorable Michael Chertoff, Secretary, Department of Homeland Security, October 27, 2005.

taking over the name-matching function through Secure Flight.[14] While these efforts may improve the accuracy in each air carrier's individual name-matching system, the improvements will only apply to their respective systems and could further exacerbate differences that currently exist among the various air carriers' systems. These differences may result in varying levels of effectiveness in the matching of passenger names against terrorist watch lists, which was a primary factor that led to the government's effort to take over the name-matching function through Secure Flight.

## Key Factors That Could Influence the Effectiveness of Secure Flight Remain to Be Finalized or Resolved

As of February 2006, several activities were under way, or were about to be decided, that would affect Secure Flight's effectiveness. For example, TSA had tested name-matching technologies to determine what type of passenger data would be needed to match against terrorist watch list data. These tests had been conducted using historical data in a controlled, rather than real-world environment, but additional testing was needed to learn more about how these technologies would perform in an operational environment. TSA also had not yet conducted stress testing to determine how the system would handle peak data volumes. Further, due to program delays and the program rebaselining, TSA had not conducted a comprehensive end-to-end testing to verify that the entire system would function as intended, although it had planned to do so by the middle of 2005.

Prior to its rebaselining effort, we further reported that TSA had not made key policy decisions for determining the passenger information that air carriers would be required to collect, the name-matching technologies that would be used to vet passenger names against terrorist watch list data, and thresholds that would be set to determine the relative volume of passengers who are to be identified as potential matches against the database. For example, TSA will need to decide which data attributes air carriers will be required to provide in passenger data to be used to match against data contained in the TSDB, such as full first, middle, and last name plus other discrete identifiers, such as date of birth. Using too many data attributes can increase the difficulty of conducting matching, while

[14] The interviews with officials from the two air carriers is part of on-going work that includes collecting information about name-matching systems currently used by air carriers to match passenger names with those on the no-fly and selectee lists in the TSDB. Information provided by the officials from the two air carriers cannot be generalized to other air carriers.

using too few attributes can create an unnecessarily high number of incorrect matches due to, among other things, the difficulty in differentiating among similar common names without further information. In addition, TSA must determine what type or combination of name-matching technologies to acquire and implement for Secure Flight, as different technologies have different capabilities. For example, earlier TSA PNR testing showed that some name-matching technologies are more capable than others at detecting significant name modifications allowing for the matching of two names that contain some variation. Detecting variation is important because passengers may intentionally make alternations to their names in an attempt to conceal their identities. In addition, unintentional variations can result from different translations of non-native names or data entry errors. TSA had planned to finalize decisions on these factors as system development progressed. However, until TSA completes its program rebaselining, data requirements for the program will remain unknown.

As we reported in February 2006, two additional factors will play an important role in the effectiveness of Secure Flight. These factors include (1) the accuracy and completeness of data contained in TSC's TSDB and in passenger data submitted by air carriers, and (2) the ability of TSA and TSC to identify false positives and resolve possible mistakes during the data-matching process to minimize inconveniencing passengers. Regarding data quality and accuracy, in a review of the TSC's role in Secure Flight, the Department of Justice Office of Inspector General found that TSC could not ensure that the information contained in its TSDB was complete or accurate. To address accuracy, TSA and TSC had planned to work together to identify false positives—passengers inappropriately matched against data contained in the terrorist-screening database—by using intelligence analysts to monitor the accuracy of data matches. Related to the accuracy of PNR data, we reported that TSA had planned to describe the required data attributes that must be contained in passenger data provided to TSA in a forthcoming rule. However, the accuracy and completeness of the information contained in the passenger data record will still be dependent on the air carriers' reservations systems, the passengers themselves, and the air carriers' modifications of their systems for transmitting the data in the proper format. Prior TSA testing found that many passenger data records submitted by air carriers were found to be inaccurate or incomplete, creating problems during the automated name-matching process.

Prior to its rebaselining effort, TSA had also reported that it planned to work with TSC to identify false positives as passenger data are matched against data in the TSDB, and to resolve mistakes to the extent possible before inconveniencing passengers. The agencies were to use intelligence analysts during the actual matching of passenger data to data contained in the TSDB to increase the accuracy of data matches. When TSA's name-matching technologies indicated a possible match, TSA analysts were to manually review all of the passenger data and other information to determine if the passenger could be ruled out as a match to the TSDB. If a TSA analyst could not rule out a possible match, the record would be forwarded to a TSC analyst to conduct a further review using additional information. Until TSA completes its rebaselining effort, it is uncertain whether this or another process will be used to help mitigate the misidentification of passengers. An additional factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's inability to identify passengers who assume the identity of another individual by committing identity theft, or who use false identifying information. Secure Flight was neither intended nor designed to address these vulnerabilities.

## Secure Flight Privacy Notices and Passenger Redress Process Cannot Be Finalized Until Program Requirements Are More Fully Defined

TSA is aware of, and plans to address, the potential for Secure Flight to adversely affect travelers' privacy and their rights. However, as we testified in February 2006, TSA, as part of its requirements development process, had not clearly identified the privacy impacts of the envisioned system or the full actions it planned to take to mitigate them. Because Secure Flight's system development documentation did not fully address how passenger privacy protections were to be met, it was not possible to assess potential system impacts on individual privacy protections, as of February 2006. Further, such an assessment will not be possible until TSA determines what passenger data will be required and how privacy protections will be addressed in the rebaselined program.

The Privacy Act and the Fair Information Practices—a set of internationally recognized privacy principles that underlie the Privacy Act—limit the collection, use, and disclosure of personal information by federal agencies.[15] TSA officials have stated that they are committed to meeting the requirements of the Privacy Act and the Fair Information Practices. However, it is not evident how this will be accomplished because TSA has not decided what passenger data elements it plans to

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

collect, how such data will be provided by stakeholders, or how a restructuring that may result from its program rebaselining will impact its requirements for passenger data. Prior to the rebaselining effort, TSA was in the process of developing but had not issued the systems-of-records notice required by the Privacy Act, or the privacy impact assessment required by the E-Government Act, that would describe how TSA will protect passenger data once Secure Flight becomes operational.[16] Moreover, privacy requirements had not been incorporated into the Secure Flight system development process to explain whether personal information would be collected and maintained in the system in a manner that complies with privacy and security requirements. In our review of Secure Flight's system requirements prior to TSA announcing its rebaselining, we found that privacy concerns were broadly defined in functional requirements documentation, which states that the Privacy Act must be considered in developing the system. However, these broad functional requirements had not been translated into specific system requirements. Until TSA determines the relevancy of these requirements and notices, privacy protections and impacts cannot be assessed.

Further, Congress mandated that Secure Flight include a process whereby aviation passengers determined to pose a threat to aviation security may appeal that determination and correct erroneous information contained within the prescreening system.[17] While TSA has not yet determined how it will meet this congressional mandate, it currently has a process in place that allows passengers who experience delays under the current prescreening conducted by air carriers to submit a passenger identity verification form to TSA and request that the agency place their names on a cleared list. If, upon review, TSA determines that the passenger's identity is distinct from the person on a watch list, TSA will add the passenger's name to its cleared list, and will forward the updated list to the air carriers. TSA will also notify the passenger of his or her cleared status and explain

[16] The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain, or disseminate information in an identifiable form. Pub. L. No. 107-347, 116 Stat. 2899.

[17] See Pub. L. Nos. 108-334, § 522(a)(1); and 109-90, § 518(a).

that in the future the passenger may still experience delays.[18] Recently, TSA has automated the cleared list process, enabling the agency to further mitigate inconvenience to travelers on the cleared list. GAO has an ongoing review examining TSA's redress process for assisting passengers misidentified under the screening program.

According to TSA officials, no final decisions have been made regarding how TSA will address redress requirements, but information on the process will be contained within the privacy notices released in conjunction with the forthcoming regulation. In May 2006, Secure Flight officials stated that concerns for privacy and redress were being addressed as part of their rebaselining effort.

## Concluding Observations

TSA has recognized the challenges it faces in developing Secure Flight and has undertaken efforts to rebaseline the program. We believe this rebaselining effort is a positive step in addressing the issues facing the program. To make and demonstrate progress on any large-scale information technology program, such as Secure Flight, an agency must first adequately define program capabilities that are to be provided, such as requirements related to performance, security, privacy, and data content and accuracy.  These requirements can then in turn be used to produce reliable estimates of what these capabilities will cost, when they will be delivered, and what mission value or benefits will accrue as a result. For Secure Flight, well-defined requirements would provide a guide for developing the system and a baseline to test the developed system to ensure that it delivers necessary capabilities, and would help to ensure that key program areas—such as security, system connectivity, and privacy and redress protections—are appropriately managed.

When we reported on Secure Flight in March 2005, TSA had committed to take action on our recommendations to manage the risks associated with developing and implementing Secure Flight, including finalizing the concept of operations, system requirements, and test plans; completing formal agreements with CBP and air carriers to obtain passenger data;

[18] In our February 2006 testimony, we stated that TSA's Office of Transportation Security Redress (OTSR) managed redress for the current watch list matching process conducted by the air carriers. At that time OTSR was developing an agency-wide policy for redress and had interviewed TSA officials as part of that effort, but found that Secure Flight requirements were not sufficiently defined for use in drafting the new policy. TSA officials stated that they would continue to discuss the Secure Flight redress process with OSTR.

developing life cycle cost estimates and a comprehensive set of critical performance measures; issuing new privacy notices; and putting a redress process in place. When we testified in February 2006, TSA had made some progress in all of these areas, including conducting further testing of factors that could influence system effectiveness and corroborating with key stakeholders. However, TSA had not completed any of the actions it had scheduled to accomplish. In particular, TSA had not developed complete system requirements or conducted important system testing, made key decisions that would impact system effectiveness, or developed a program management plan and a schedule for accomplishing program goals.

In conjunction with its rebaselining effort, TSA has taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program director to administer Secure Flight and a program manager with information systems program management credentials. We support these efforts and believe that proceeding with operational testing and completing other key program activities should not be pursued until TSA demonstrates that it has put in place a more disciplined life cycle process as part of its rebaselining effort.

Mr. Chairman, this concludes my prepared statement. I will be pleased to respond to any questions that you or other members of the committee have at the appropriate time.

## GAO Contacts and Staff Acknowledgments

For further information about this testimony, please contact Cathleen Berrick, at 202-512-3404 or at berrickc@gao.gov, or Randolph C. Hite at 202-512-6256 or at hiter@gao.gov.

Other key contributors to this statement were J. Michael Bollinger, Amy Bernstein, Mona Nichols Blake, Christine Fossett, and Allison G. Sands.

# Appendix I: Related GAO Products

*Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*. GAO-06-374T. Washington, D.C.: February 9, 2006.

*Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*. GAO-05-864R. Washington, D.C.: July 22, 2005.

*Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*. GAO-05-356 Washington, D.C.: March 28, 2005.

*TSA's Modifications to Rules for Prescreening Passengers*. GAO-05-445SU Washington D.C.: March 28, 2005.

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

*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.

*Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*. GAO-04-385 Washington, D.C.: February 12, 2004.

# Appendix II: Legislatively Mandated Secure Flight Issues to be Certified by DHS and Reviewed by GAO

| Legislative mandated issue (short title) | Description of mandated issue |
|---|---|
| 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 TSA may appeal such decisions and correct erroneous information contained in CAPPS II or Secure Flight or other follow-on/successor programs. |
| 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. |
| Stress testing | TSA has stress-tested and demonstrated the efficacy and accuracy of all search technologies 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. |
| 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. |
| Operational safeguards | TSA has built in sufficient operational safeguards to reduce the opportunities for abuse. |
| 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. |
| Oversight of system use and operation | TSA has adopted policies establishing effective oversight of the use and operation of the system. |
| Privacy concerns | There are no specific privacy concerns with the technological architecture of the system. |

| Legislative mandated issue (short title) | Description of mandated issue |
|---|---|
| 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. |
| Life cycle cost estimates and expenditure plans | Appropriate life cycle cost estimates and expenditure and program plans exist. |

Source: GAO.

# Appendix III: Scope and Methodology

The results discussed in this testimony are based on our review of available documentation on Secure Flight's systems development and oversight, policies governing program operations, our past reports on the program, and interviews with Department of Homeland Security officials, TSA program officials and their contractors, and other federal officials who are key stakeholders in the Secure Flight program. Throughout our ongoing reviews of Secure Flight, we have reviewed TSA's System Development Life Cycle Guidance for developing information technology systems and other federal reports describing best practices in developing and acquiring these systems. We also reviewed draft TSA documents containing information on the development and testing of Secure Flight, including concept of operations, requirements, test plans, and test results. We also reviewed reports from the U.S. Department of Justice Office of the Inspector General that reviewed the Secure Flight program and reports from two oversight groups that provided advisory recommendations for Secure Flight: DHS's Privacy and Data Integrity Advisory Committee and TSA's Aviation Security Advisory Committee Secure Flight Working Group. We interviewed senior-level TSA officials, including representatives from the Office of Transportation Threat Assessment and Credentialing, which is responsible for Secure Flight, and the Office of Transportation Security Redress, to obtain information on Secure Flight's planning, development, testing, and policy decisions. We also interviewed representatives from the U.S. Customs and Border Protection and Terrorist Screening Center[1] to obtain information about stakeholder coordination. We also interviewed officials from several air carriers and representatives from aviation trade organizations regarding issues related to Secure Flight's development and implementation. In addition, we attended conferences on name-matching technologies sponsored by MITRE (a federally funded research and development corporation) and the Office of the Director of National Intelligence.

[1] TSC was established in accordance with Homeland Security Presidential Directive-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.

This testimony includes work accomplished for our March 2005 report[2] and our February 2006 testimony,[3] and work conducted from February 2006 to June 2006 in accordance with generally accepted government auditing standards.

[2] GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: February 9, 2006).

[3] GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, GAO-05-356 (Washington, D.C.: March 2005).

## 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