United States Government Accountability Office

GAO

Testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, February 9, 2006

AVIATION SECURITY

Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program

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

GAO
Accountability * Integrity * Reliability

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-374T a report to the Committee on Commerce, Science, and Transportation, U.S. Senate

February 9, 2006

AVIATION SECURITY

Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program

Why GAO Did This Study

After the events of September 11, 2001, Congress created the Transportation Security Administration (TSA) and directed it to assume 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 is 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. This testimony includes information on areas of congressional interest that GAO has previously reported on.

What GAO Recommends

In a prior report, GAO 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 and 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 plans to take.

www.gao.gov/cgi-bin/getrpt?GAO-06-374T.

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 has made some progress in developing and testing the Secure Flight program. However, TSA has not followed a disciplined life cycle approach to manage systems development, or fully defined system requirements. Rather, TSA has followed a rapid development method intended to develop the program quickly. This process has been ad hoc, resulting in project activities being conducted out of sequence, requirements not being fully defined, and documentation containing contradictory information or omissions. Further, while TSA has taken steps to implement an information security management program for protecting information and assets, its efforts are incomplete. Finally, TSA is proceeding to develop Secure Flight without a program management plan containing program schedule and cost estimates. Oversight reviews of the program have also raised questions about program management. Without following a more rigorous and disciplined life cycle process, including defining system requirements, the Secure Flight program is at serious risk of not meeting program goals.

Over the past year, TSA has made some progress in managing risks associated with developing Secure Flight, and has recently taken actions that recognize the need to instill more rigor and discipline into the development process. TSA has also 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 need more definitive information about system requirements from TSA to plan for their support of the program.

In addition, several activities that will affect Secure Flight's effectiveness are under way, or have not yet been decided. For example, TSA conducted name-matching tests, which compared passenger and terrorist screening database data, to evaluate the ability of the system to function. However, TSA has not yet made key policy decisions which could significantly impact program operations, including what passenger data it will require air carriers to provide and the name-matching technologies it will use.

Further, Secure Flight's system development documentation does not fully explain how passenger privacy protections are to be met, and TSA has not issued the privacy notices that describe how it will protect passenger data once Secure Flight becomes operational. As a result, it is not possible to assess how TSA is addressing privacy concerns. TSA is also determining how it will provide for redress, as mandated by Congress, to provide aviation passengers with a process to appeal determinations made by the program and correct erroneous information contained within the prescreening process. However, TSA has not finalized its redress polices.

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) Secure Flight program. 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 presents information on the progress TSA has made and the challenges it faces in (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.

My testimony is based on our past reviews of the Secure Flight program, and on 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 congressional committees.[1] (See app. 1 for a description of the 10 issues.) My testimony today updates information presented in our March 2005 report on the status of Secure Flight's development and implementation,[2] including 9 of the 10 areas of

[1] 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.

[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 interest.[3] 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.

Today, I present information that suggests that, 3 years after TSA began developing a program to provide passenger prescreening, significant challenges remain in developing and implementing the Secure Flight program. The results I am presenting are based on our review of available documentation on Secure Flight's systems development and oversight, policies governing program operations, and our past reports on the program, and interviews with Department of Homeland Security (DHS) officials, TSA program officials and their contractors, and other federal officials who are key stakeholders in the Secure Flight program. We 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. My testimony is based on TSA documents received, but does not necessarily reflect all documentation that was only recently made available. In addition to the TSA documents we have reviewed, we also reviewed reports from the U.S. Department of Justice Office of the Inspector General (DOJ-OIG), which 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 Analysis and Credentialing, which is responsible for Secure Flight, and the Office of Transportation Security Redress (OTSR), to obtain

[3] This statement does not provide information on the area of congressional interest related to modifications with respect to intrastate travel to accommodate states with unique air transportation needs because data were not yet available to us on the effect of these modifications on air carriers.

information on Secure Flight's planning, development, testing, and policy decisions. We also interviewed representatives from the U.S. Customs and Border Protection (CBP) and Terrorist Screening Center (TSC)[4] to obtain information about stakeholder coordination. We also interviewed officials from an air carrier 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. Our work was conducted from April 2005 to February 2006 in accordance with generally accepted government auditing standards.

Summary

In developing and managing the Secure Flight program, TSA has not conducted critical activities in accordance with best practices for large-scale information technology programs. Specifically, TSA has 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 have 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 has 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, has 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 systems interconnect, and how system security is achieved. We found that Secure Flight's requirements documentation contained contradictory and missing information. TSA officials have acknowledged that they have not followed a disciplined life cycle approach in developing Secure Flight, and stated that they are currently rebaselining the program to follow their standard Systems Development

[4] 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.

Life cycle process, including defining system requirements. We also found that while TSA has taken steps to implement an information security management program for protecting Secure Flight information and assets, its efforts are incomplete, based on federal standards and industry best practices. 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. Finally, TSA is proceeding with Secure Flight development without an effective program management plan that contains current program schedules and cost estimates. TSA officials stated they have not maintained an updated schedule in part because the agency has not yet 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 can impact when Secure Flight will be operational and at what cost. While we recognize 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. Further, several oversight reviews of the program have been conducted and raise questions about program management, including the lack of fully defined requirements. TSA has recently taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program manager with information systems program management credentials, and more completely defining system requirements and a program management plan, including the development of schedules and cost estimates.

TSA has 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 for Secure Flight operations, but additional information and testing are needed to enable stakeholders to provide the necessary support for the program. TSA has, for example, drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and has begun receiving feedback from the air carriers on this information. TSA is also in the early stages of coordinating with U.S. Customs and Border Protection and the federal Terrorist Screening Center on broader issues of integration and interoperability related to other people-screening programs used by the government to combat terrorism. In addition, TSA has conducted preliminary network connectivity testing between TSA and federal stakeholders to determine, for example, how information will 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 is not possible to conduct stress testing to determine if the system can handle the volume of data traffic that will be required by Secure Flight. TSA acknowledged it has not determined what the real data volume requirements will be, and cannot do so until the regulation for air carriers has been issued and their data management role has been finalized. All key program stakeholders also stated that additional information is needed before they can finalize their plans to support Secure Flight operations. A TSC official stated, for example, that until TSA provides estimates of the volume of potential name matches that TSC will be required to screen, TSC cannot make decisions about required resources. Also, ongoing coordination of prescreening and name-matching initiatives with CBP and TSC can impact how Secure Flight is implemented.

In addition to collaborating with stakeholders, TSA has, over the past 11 months, made some progress in evaluating factors that could influence system effectiveness. However, several activities are under way, or are to be decided, that will also affect Secure Flight's effectiveness, including operational testing to provide information about Secure Flight's ability to function. TSA has been testing name-matching technologies to determine what type of passenger data will be needed to match against terrorist watch list data. These tests have been conducted thus far in a controlled, rather than real-world environment, using historical data, but additional testing is needed to learn more about how these technologies will perform in an operational environment. In addition, due to program delays, TSA has not yet conducted comprehensive end-to-end testing to verify that the entire system functions as intended, although it had planned to do so last summer. TSA also has not yet conducted stress testing to determine how the system will handle peak data volumes. In addition, TSA has not made key policy decisions for determining the passenger information that air carriers will be required to collect, the name-matching technologies that will be used to vet passenger names against terrorist watch list data; and thresholds that will be set to determine the relative volume of passengers who are to be identified as potential matches against the database. TSA plans to finalize decisions on these factors as system development progresses. However, until these decisions are made, data requirements will remain unsettled and key stakeholders—in particular, air carriers—will not have the information they need to assess and plan for needed changes to their systems to interface with Secure Flight. On the issue of data quality and accuracy, while the completeness and accuracy of data contained in the government's terrorist screening database can never be certain—given the varying quality of intelligence information gathered, and changes in this information over time—TSC has established some processes to help ensure the quality of these data. However, 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 databases was complete or accurate. According to a TSC official, TSA and TSC plan to enter into a letter of agreement that will describe the data elements from the terrorist-screening database, among other things, to be used for Secure Flight. To address accuracy, TSA and TSC plan 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. 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 is neither intended to nor designed to address these vulnerabilities.

Because Secure Flight's system development documentation does not fully address how passenger privacy protections are to be met, it is not possible to assess potential system impacts on individual privacy protections. 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. 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 yet evident how this will be accomplished because TSA has not decided what passenger data elements it plans to collect, or how such data will be provided by stakeholders. Further, TSA is in the process of developing but has not issued the systems of records notice, which is required by the Privacy Act, or the privacy impact assessment, which is required by the E-Government Act, that would describe how TSA will protect passenger data once Secure Flight becomes operational. Moreover, privacy requirements were not incorporated into the Secure Flight system development process in a manner that would explain whether personal information will 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, 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 have not been translated into specific system requirements. TSA officials stated that they are completing work on integrating privacy and requirements into the Secure Flight system as the program is being developed, and that new privacy notices will be issued in conjunction with a forthcoming regulation prior to proceeding with the system's initial operating capability. Until TSA finalizes these requirements and notices, however, privacy protections and impacts cannot be assessed. TSA is also determining how it will meet a congressional mandate that the Secure Flight program 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. According to TSA officials, no final decisions have been made regarding how TSA will address the redress requirements, but information on the process will be contained within the privacy notices released in conjunction with the forthcoming regulation.

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.[5]

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,[6] 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

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

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

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.

Based in part on concerns about privacy and other issues expressed by us and others, DHS canceled the development of CAPPS II in August 2004 and shortly thereafter 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. Secure Flight will operate on the Transportation Vetting Platform (TVP)[7]—the underlying infrastructure (hardware and software) to support the Secure Flight application, including security, communications, and data management; and, the Secure Flight application is 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 is also to be configurable—meaning that it can be quickly adjusted to reflect changes to workflow parameters. Aspects of Secure Flight are currently undergoing development and testing, and policy decisions regarding the operations of the program have not been finalized.[8]

Overview of Secure Flight Operations

As currently envisioned, under Secure Flight, when a passenger makes flight arrangements, the organization accepting the reservation, such as the air carrier's reservation office or a travel agent, will enter passenger name record (PNR) information obtained from the passenger, which will

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

[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)).

then be stored in the air carrier's reservation system.[9] While the government will be asking for only portions of the PNR, the PNR data can 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 will be sent to Secure Flight through a network connection provided by DHS's CBP. Reservations or changes to reservations that are made less than 72 hours prior to flight time will be sent immediately to TSA through CBP.

Upon receipt of passenger data, TSA plans to process the passenger data through the Secure Flight application running on the TVP. During this process, Secure Flight is to determine if the passenger data match 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 will 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 plans to provide TSA with an extract of the TSDB for use in Secure Flight, and provide updates as they occur. This TSDB subset will 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 will be denied boarding unless they are cleared by law enforcement personnel).[11] To perform the match, Secure Flight is to compare the passenger, TSDB, and other watch list data using automated name-matching technologies. When a possible match is generated, TSA and potentially TSC analysts will conduct a manual review comparing additional law enforcement and other government information with passenger data to determine if the person can be ruled out as a possible

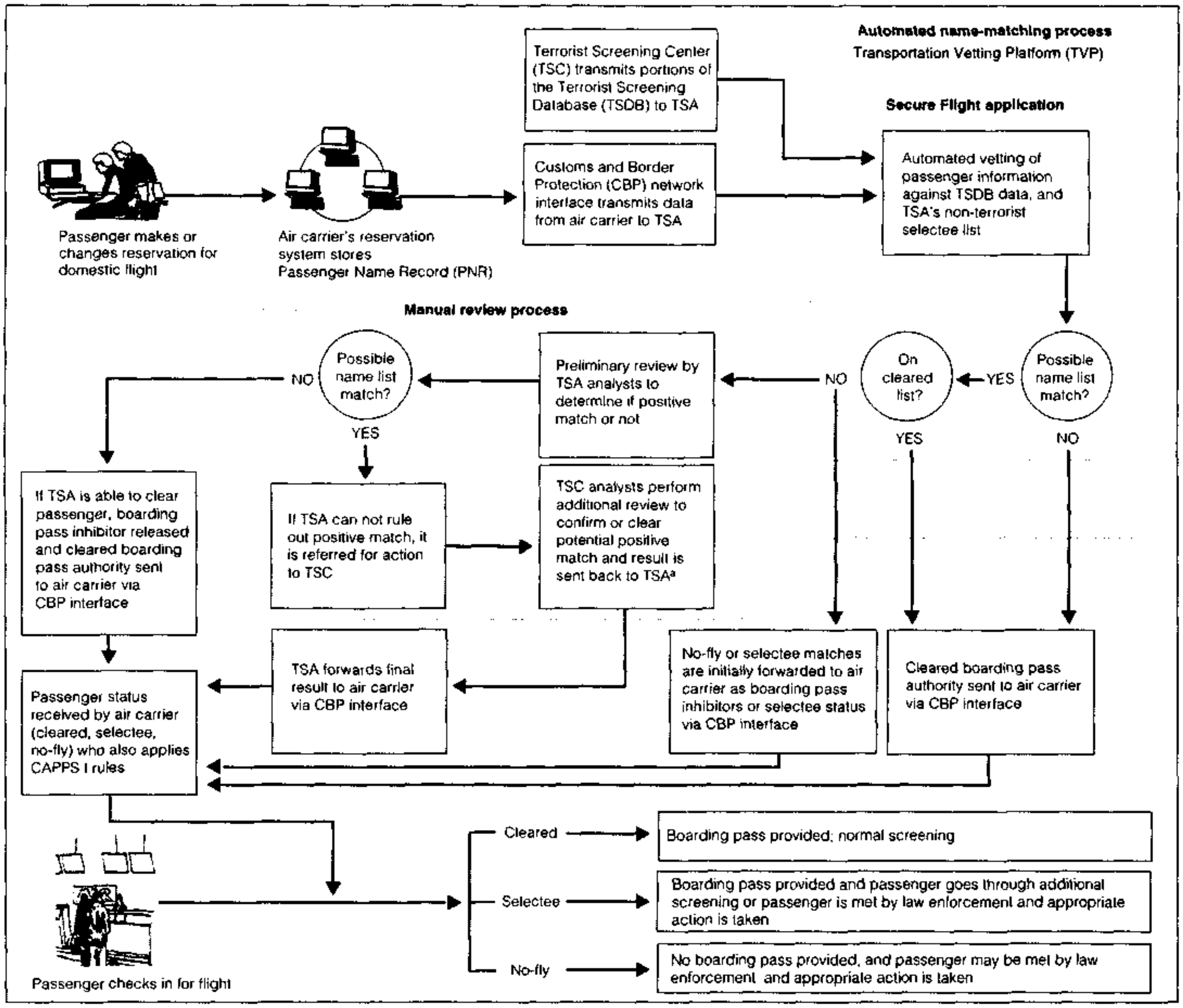
[9] This description of the Secure Flight system, as well as the graphic illustrating the system in figure1, is based on TSA's draft June 9, 2005, concept of operations, a document that gives a high-level overview of the Secure Flight system.

[10] TSA also plans to utilize a cleared list as part of the watch list matching process; the cleared list is 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.

match. TSA is to return the matching results to the air carriers through CBP. Figure 1 illustrates how Secure Flight is intended to operate.

Figure 1: Planned Operation of Secure Flight


Automated name-matching process
Transportation Vetting Platform (TVP)
Terrorist Screening Center (TSC) transmits portions of the Terrorist Screening Database (TSDB) to TSA
Secure Flight application
Automated vetting of passenger information against TSDB data, and TSA's non-terrorist selectee list
Customs and Border Protection (CBP) network interface transmits data from air carrier to TSA
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
Passenger checks in for flight
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

Source: GAO analysis of TSA data.

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

As shown in figure 1, when the passenger checks in for the flight at the airport, the passenger is to receive a level of screening based on his or her designated category. A cleared passenger is to be provided a boarding pass and allowed to proceed to the screening checkpoint in the normal manner. A selectee passenger is to receive additional security scrutiny at the screening checkpoint.[12] 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 Has Not Followed a Disciplined Life Cycle Approach or Fully Defined System Requirements, Schedule, and Costs

TSA has not followed a disciplined life cycle approach in developing Secure Flight, in accordance with best practices for large-scale information technology programs. Following a disciplined life cycle, activities and related documentation are to be developed in a logical sequence. TSA also has not finalized and documented functional and system requirements that fully link to each other and to source documents. Without adequately defined requirements, TSA cannot finalize a system security plan or develop a reliable program schedule or life cycle cost estimates. In addition to these concerns, other reviews that have been conducted of Secure Flight have raised questions about the management of the program.

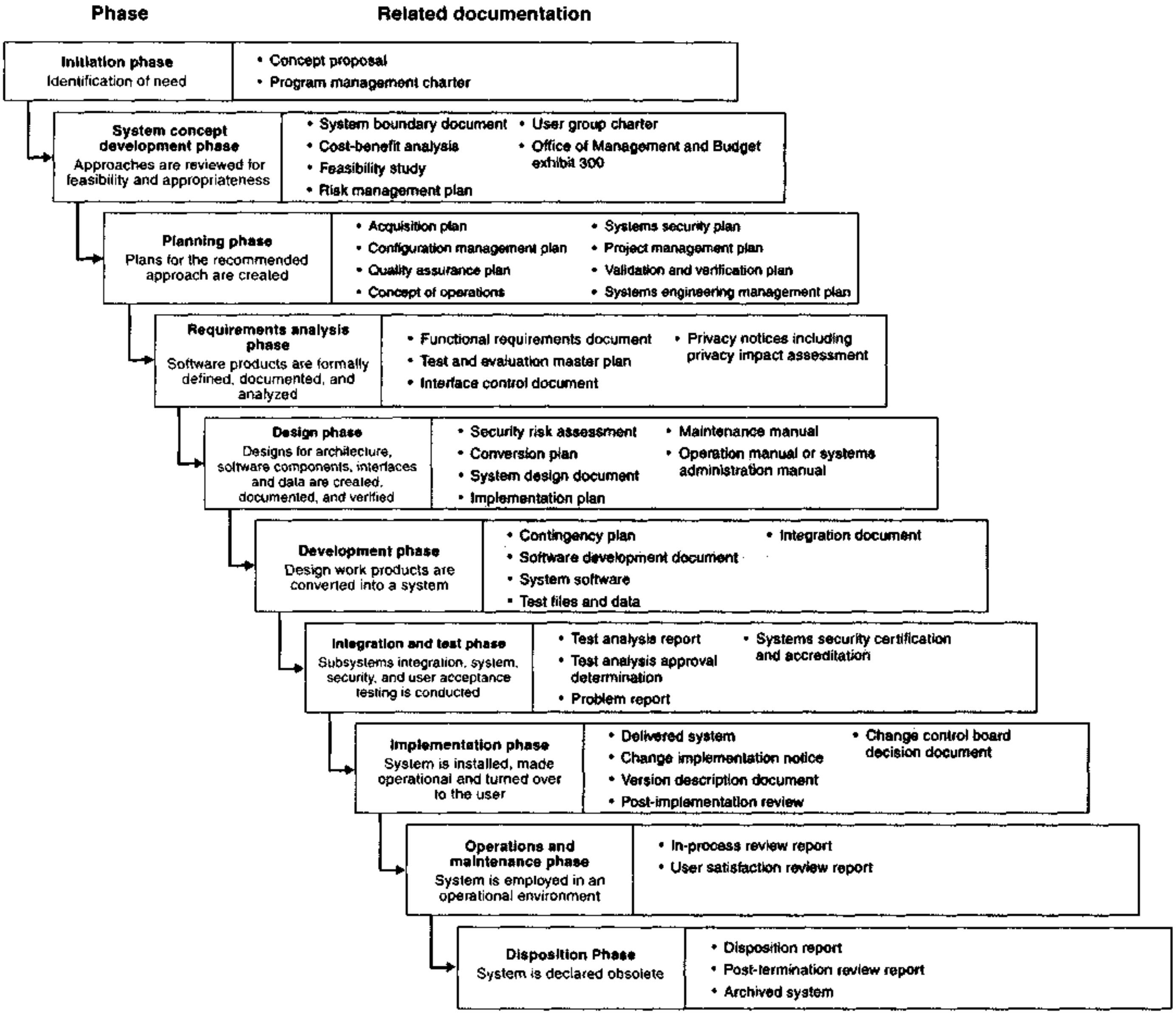
TSA Has Not Followed a Disciplined Life Cycle Process or Fully Defined System Requirements but Plans to Address These Issues

Based on evaluations of major federal information technology programs like Secure Flight, and research by others, following a disciplined life cycle management process in which key activities and phases of the project are conducted in a logical and orderly process and are fully documented, helps ensure that programs achieve intended goals within acceptable levels of cost and risk. Such a life cycle process begins with initial concept definition and continues through requirements determination to final testing, implementation, and maintenance. TSA has established a System Development Life Cycle (SDLC) that defines a series of orderly phases and

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

associated steps and documentation. The SDLC serves as the mechanism to ensure that systems are effectively managed and overseen. Figure 2 provides a description of TSA's SDLC phases and related documentation.

Figure 2: Summary of TSA's System Development Life Cycle Process



Phase	Related documentation
Initiation phase Identification of need	• Concept proposal • Program management charter
System concept development phase Approaches are reviewed for feasibility and appropriateness	• System boundary document • Cost-benefit analysis • Feasibility study • Risk management plan • User group charter • Office of Management and Budget exhibit 300
Planning phase Plans for the recommended approach are created	• Acquisition plan • Configuration management plan • Quality assurance plan • Concept of operations • Systems security plan • Project management plan • Validation and verification plan • Systems engineering management plan
Requirements analysis phase Software products are formally defined, documented, and analyzed	• Functional requirements document • Test and evaluation master plan • Interface control document • Privacy notices including privacy impact assessment
Design phase Designs for architecture, software components, interfaces and data are created, documented, and verified	• Security risk assessment • Conversion plan • System design document • Implementation plan • Maintenance manual • Operation manual or systems administration manual
Development phase Design work products are converted into a system	• Contingency plan • Software development document • System software • Test files and data • Integration document
Integration and test phase Subsystems integration, system, security, and user acceptance testing is conducted	• Test analysis report • Test analysis approval determination • Problem report • Systems security certification and accreditation
Implementation phase System is installed, made operational and turned over to the user	• Delivered system • Change implementation notice • Version description document • Post-implementation review • Change control board decision document
Operations and maintenance phase System is employed in an operational environment	• In-process review report • User satisfaction review report
Disposition Phase System is declared obsolete	• Disposition report • Post-termination review report • Archived system

Source: GAO analysis.

TSA has not followed its SDLC in developing and managing Secure Flight. Rather, program officials stated that they have used a rapid development method that was intended to enable them to develop the program more quickly. However, these officials could not provide us with details on how this approach was implemented. As a result, our analysis of steps performed and documentation developed indicates that Secure Flight has not been pursued within the context of a logical, disciplined, system development methodology. Rather the process has been ad hoc, with project activities conducted out of sequence. For example, program officials declared that the program's design phase was completed before system requirements had been adequately detailed, and key activities have yet to be adequately performed, such as program planning and defining system requirements. TSA officials acknowledged that problems arose with Secure Flight as a result of using this approach. As a result, it is currently unclear what Secure Flight capabilities are to be developed, by when, at what cost, and what benefits are to accrue from the program. Without clarification on these decision points, the program is at risk of failure.

Defining and documenting system requirements is integral to life cycle development. Based on best practices and our prior work in this area, the expected capabilities of a system such as Secure Flight should be defined in terms of requirements for functionality (what the system is to do), performance (how well the system is to execute functions), data (what data are needed by what functions, when, and in what form), interface (what interactions with related and dependent systems are needed), and security. Further, system requirements should be unambiguous, consistent with one another, linked (that is, traceable from one source level to another),[13] verifiable, understood by stakeholders, and fully documented.

TSA has prepared certain Secure Flight requirements documents, and officials stated that they are now reviewing those requirements

[13] Examples of higher-order sources include legislation, which may dictate certain requirements, and other system documentation, such as the operational concept. When requirements are managed well, traceability can be established from the source requirements to lower-level requirements and from the lower level back to their source. Such bidirectional traceability helps determine that all source requirements have been addressed completely and that all lower-level requirements can be verified as derived from a valid source.

documents.[14] We support these review efforts because we found, in the requirements documents we reviewed, inconsistencies and ambiguities in requirements documentation for system functions, performance, data, and security—and that these documents were not always complete. For example, according to TSA's SDLC guidance and best practices for developing information technology systems, systems like Secure Flight should have a comprehensive concept of operations covering all aspects of the program during the planning phase (see fig. 2). We reported in our March 2005 report that TSA had not yet finalized a concept of operations, which would describe conceptually the full range of Secure Flight operations and interfaces with other systems, and we recommended that it develop one. Since March 2005, TSA documents refer to numerous concept of operations, such as a long concept of operations, a short concept of operations, and an initial operational capability concept of operations. TSA provided a June 2005 concept of operations for our review, but this document does not contain key system requirements, such as the high-level requirements for security and privacy.

In addition, we found that Secure Flight requirements were unclear or missing. For example, while the requirements that we reviewed state that the system be available 99 percent of the time, this only covers the TVP and Secure Flight application. It does not include requirements for the interfacing systems critical for Secure Flight operations. Thus, the availability requirements for all of the components of the Secure Flight system are not yet known. Some data requirements are also vague or incomplete; for example, one data requirement is that the data is current, but the meaning of current is not defined. In addition, only some system security requirements are identified in the security document provided to us for the TVP, and sections in TSA's Systems Requirements Specification contain only placeholder notes—"to be finalized"—for security and privacy requirements.

TSA officials acknowledged that it is important that requirements be traceable to ensure that they are consistently, completely, and correctly defined, implemented, and tested. To help accomplish this, TSA officials

[14] Key requirements documentation we reviewed included the Transportation Vetting Platform/Secure Flight System Requirements Specification (May 13, 2005), the Secure Flight System Security Plan (July 15, 2005), the Transportation Vetting Platform System Security Plan (July 15, 2005), Transportation Vetting Platform and Secure Flight Security Risk Assessment (July 15, 2005), and documentation called for under Federal Information Processing Standard (FIPS) 199 (August 23, 2005).

stated that they use a requirements tracking tool for Secure Flight that can align related requirements to different documents, and thus establish traceability (e.g., it can map the Systems Requirements Specification to a functional requirements document). According to program officials, this tool can also be used for aligning and tracing requirements to test cases (i.e., scenarios used to determine that the system is working as intended). We found, however, that requirements for Secure Flight have not been fully traced. For example, we were not able to trace system capabilities in contractual documents to the concept of operations and then to the various requirement documents, to design phase use cases, and to test cases. In addition, contractor staff we interviewed stated that they were unable to use this tool to align or trace necessary requirements without the aid of supplemental information. Without internal alignment among system documentation relating to requirements, there is not adequate assurance that the system produced will perform as intended.

In addition, we found that available Secure Flight requirements documents did not define the system's boundaries, including interfaces, for each of the stakeholders—that is, the scope of the system from end to end, from an air carrier to CBP, to TSA, to TSC, and back to TSA, then again to CBP and air carriers (refer to fig. 1 for an overview of this process). Defining a system's boundaries is important in ensuring that system requirements reflect all of the processes that must be executed to achieve a system's intended purpose. According to TSA's SDLC guidance, a System Boundary Document is to be developed early in the system life cycle. However, in its third year of developing a passenger prescreening system, TSA has not yet prepared such a document. Although the System Boundary Document was not available, the program's Systems Security Document does refer to an "accreditation boundary," which defines the Secure Flight system from the standpoint of system security accreditation and certification. According to this definition of what Secure Flight includes, those systems that are needed to accomplish Secure Flight program goals (e.g., those of commercial air carriers, CBP, and TSC) are not part of Secure Flight. If the boundary documents, and thus the requirements, do not reflect all system processes and connections that need to be performed, the risk is increased that the system will not achieve Secure Flight's intended purpose. Moreover, until all system requirements have been defined, TSA will not be able to stress-test Secure Flight in an operational, end-to-end mode. In our March 2005 report, we recommended that TSA finalize its system requirements documents and ensure that these documents address all system functionality. Although TSA agreed with our recommendations, the requirements documentation that we reviewed showed that the agency has not yet completed these activities.

Our evaluations of major federal information technology programs, and research by others, has shown that following a disciplined life cycle management process decreases the risks associated with acquiring systems. The steps and products in the life cycle process each have important purposes, and they have inherent dependencies among themselves. Thus, if earlier steps and products are omitted or deficient, later steps and products will be affected, resulting in costly and time-consuming rework. For example, a system can be effectively tested to determine whether it meets requirements only if these requirements have already been fully defined. Concurrent, incomplete, and omitted activities in life cycle management exacerbate the program risks. Life cycle management weaknesses become even more critical as the program continues, because the size and complexity of the program will likely only increase, and the later problems are found, the harder and more costly they will likely be to fix.

In October 2005, Secure Flight's director of development stated in a memorandum to the assistant TSA administrator responsible for Secure Flight that by not following a disciplined life cycle approach, in order to expedite the delivery of Secure Flight, the government had taken a calculated risk during the requirements definition, design, and development phases of the program's life cycle development. The director stated that by prioritizing delivery of the system by a specified date in lieu of delivering complete documentation, TSA had to lower its standards of what constituted acceptable engineering processes and documentation. Since then, TSA officials stated that the required system documentation associated with each phase of the TSA life cycle is now being developed to catch up with development efforts. In addition, TSA recognized that it faces challenges preparing required systems documentation, and to help in this regard it has recently hired a certified systems program manager to manage systems development. In January 2006, this program manager stated that as Secure Flight moves forward, TSA's SDLC would be followed in order to instill greater rigor and discipline into the system's development. In addition, TSA plans to hire a dedicated program director for Secure Flight to manage program activities, schedules, milestones, costs, and program contractors, among other things.

Comprehensive System Security Management Program Has Not Yet Been Established in Accordance with Federal Guidance

TSA has taken steps to implement an information system security management program for protecting Secure Flight information and assets. Secure Flight's security plans and the related security review, which TSA developed and conducted to establish authority to operate, are important steps in the system's development. However, the steps related to system security TSA has taken to date are individually incomplete, and collectively fall short of a comprehensive system security management program. Federal guidance and industry best practices describe critical elements of a comprehensive information system security management program. Without effective system security management, it is unlikely that Secure Flight will, for example, be adequately protected against unauthorized access and use, disruption, modification, and destruction.

According to National Institute of Standards and Technology (NIST)[15] and Office of Management and Budget (OMB) guidance under the Federal Information Security Management Act, as well as industry best practices, a comprehensive system security management program includes (1) conducting a system wide risk assessment that is based on system threats and vulnerabilities, (2) developing system security requirements and related policies and procedures that govern the operation and use of the system and address identified risks, (3) certifying that the system is secure based on sufficient review and testing to demonstrate that the system meets security requirements, and (4) accrediting the system as secure in an operational setting.

TSA has developed two system security plans—one for the TVP and one for the Secure Flight application. However, neither of these plans nor the security activities that TSA has conducted to date are complete. For example, while security threats and vulnerabilities were assessed in the documentation and risks were identified in risk assessments, requirements to address these risks were only partially defined in the security plan for the TVP, and they were not included at all in the plan for the Secure Flight application. In addition, the sections on security requirements and privacy requirements in the System Requirements Specification document read "to be finalized" with no further description.

[15] The NIST requirements provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal governments. The guidelines apply to all components of an information system that processes, stores, or transmits federal information.

Moreover, we also found that the security systems plans did not reflect the current level of risk designated for the program. For example, although the July 15, 2005, System Security Plan for the TVP arrived at an overall assessment of its exposure to risks as being "medium," an August 23, 2005, requirements document found that the security risk level for the TVP was "high." As a system moves from a medium to a high level of risk, the security requirements become more stringent. TSA has not provided us with an updated System Security Plan for the TVP that addressed this greater level of risk by including additional NIST requirements for a high-risk system. In addition, this TVP System Security Plan included only about 40 percent of the NIST requirements associated with a medium-risk system. Without addressing all NIST requirements, in addition to those required for a high-risk system, TSA may not have proper controls in place to protect sensitive information.

According to federal guidance and requirements, the determination and approval of the readiness of a system to securely operate is accomplished via a certification and accreditation process. On September 30, 2005, the TSA assistant administrator responsible for Secure Flight formally granted authority, based on certification and accreditation results, for the TVP and the Secure Flight application to operate.[16] However, the team performing the certification found that TSA was unsure whether they tested all components of the security system for the TVP and the Secure Flight application, because TSA lacked an effective and comprehensive inventory system. Therefore the certification team could not determine whether its risk assessments were complete or accurate. This team also documented 62 security vulnerabilities for the Secure Flight application and 82 security vulnerabilities for the TVP. The certification team recommended authority to operate on the condition that corrective action or obtaining an exemption for the identified vulnerabilities would be taken within 90 days or the authority to operate would expire. TSA officials stated that these vulnerabilities had been addressed except for three that are being reviewed in a current security audit.

[16] An authorization to operate is issued for the information system, if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is acceptable.

Program Management Plan and Supporting Schedules and Cost Estimates for Secure Flight Have Not Been Maintained

TSA has proceeded with Secure Flight development over the past year without a complete and up-to-date program management plan, and without associated cost and schedule estimates showing what work will be done by whom, at what cost, and when. A program management plan can be viewed as a central instrument for guiding program development. Among other things, the plan should include a breakout of the work activities and products that are to be conducted in order to deliver a mission capability to satisfy stated requirements and produce promised mission results. This information, in turn, provides the basis for determining the time frames and resources needed for accomplishing this work, including the basis for milestones, schedules, and cost estimates. TSA has not provided us with either the complete and up-to-date program management plan, or an estimated schedule and costs for Secure Flight. According to a TSA official, an updated program management plan is currently being developed and is about 90 percent complete.

In lieu of a program management plan with a schedule and milestones, TSA has periodically disclosed program milestones. However, the basis for and meaning of these milestones have not been made clear, and TSA's progress in meeting these milestones has not been measured and disclosed. TSA's SDLC and OMB[17] guidance require that programs like Secure Flight provide risk-adjusted schedule goals, including key milestones, and that programs demonstrate satisfactory progress toward achieving their stated performance goals. In March 2005, we reported that the milestone that TSA set for achieving initial operating capability for Secure Flight had slipped from April 2005 to August 2005. TSA officials stated that TSA revised this milestone to state that instead of achieving initial operating capability, it would begin operational testing. This new milestone subsequently slipped first to September 2005, then to November 2005. Since that time, the program has not yet begun operational testing or initial operations, and TSA has not yet produced an updated schedule identifying when program operations will begin or when other key milestones are to be achieved to guide program development and implementation. Further, while agency officials stated that they are now planning for operational testing of an unspecified capability, no milestone date has been set for doing so.

[17] OMB, Circular No. A-11, Part 7, Sec. 300. *Planning, Budgeting, Acquisition, and Management of Capital Assets.*

TSA officials stated that they have not maintained an updated program schedule for Secure Flight in part because the agency has not yet determined the rulemaking approach it will pursue for requiring commercial air carriers to submit certain passenger data needed to operate Secure Flight, among other things. Specifically, TSA officials stated that a schedule with key milestones, such as operational testing, cannot be set until after air carriers have responded to the rulemaking and provided their plans and schedules for participating in Secure Flight. The rulemaking has been pending since the spring of 2005, and the rule remains in draft form and is under review, according to TSA officials. Once the rule has been issued, TSA officials stated that air carriers will be given time to respond with their plans and schedules. TSA officials further stated that until this occurs, and a decision is made as to how many air carriers will participate in a yet-to-be-defined initial phase of the program (they are expected to begin incrementally), a program schedule cannot be set.

Further, TSA has not yet established cost estimates for developing and deploying either an initial or a full operating capability for Secure Flight, and it has not developed a life-cycle cost estimate (estimated costs over the expected life of a program, including direct and indirect costs and costs of operation and maintenance). TSA also has not updated its expenditure plan—plans that generally identify near-term program expenditures—to reflect the cost impact of program delays, estimated costs associated with obtaining system connectivity with CBP, or estimated costs expected to be borne by air carriers. Program and life cycle cost estimates are critical components of sound program management for the development of any major investment. Developing cost estimates is also required by OMB guidance and can be important in making realistic decisions about developing a system. Expenditure plans 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.

In our March 2005 report, we recommended that TSA develop reliable life cycle cost estimates and expenditure plans for the Secure Flight program, in accordance with guidance issued by OMB, in order to provide program managers and oversight officials with the information needed to make informed decisions about program development and resource allocations. Although TSA agreed with our recommendation, it has not yet provided this information. TSA officials stated that developing program and life cycle cost estimates for Secure Flight is challenging because no similar programs exist from which to base cost estimates and because of the uncertainties surrounding Secure Flight requirements. Further, they stated that cost estimates cannot be accurately developed until after system testing is completed and policy decisions have been made regarding Secure Flight requirements and operations. Notwithstanding these statements, TSA officials stated that they are currently assessing program and life cycle costs as part of their rebaselining and that this new baseline will reflect updated cost, funding, scheduling, and other aspects of the program's development.

While we recognize that program unknowns introduce uncertainty into the program-planning process, including estimating tasks, time frames, and costs, 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. In program planning, assumptions need to be made and disclosed in the plans, along with the impact of the associated uncertainty on the plans and estimates. As more information becomes known over the life of the program, these plans should be updated to recognize and reflect the greater confidence in activities that can be expressed with estimates.

Program management plans and related schedules and cost estimates—based on well-defined requirements—are important in making realistic decisions about a system's development, and can alert an agency to growing schedule or cost problems and the need for mitigating actions. Moreover, best practices and related federal guidance emphasize the need to ensure that programs and projects are implemented at acceptable costs and within reasonable and expected time frames. Investments such as Secure Flight are approved on the expectation that programs and projects will meet certain commitments to produce certain capabilities and benefits (mission value) within the defined schedule and cost. Until an updated program management plan and related schedules and cost estimates and expenditure plans, are prepared for Secure Flight—which should be developed despite program uncertainties, and updated as more information is gained—TSA and Congress will not be able to provide complete oversight over the program's progress in meeting established commitments.

Oversight Reviews of Secure Flight Have Been Conducted and Raised Questions about Program Management

DHS and TSA have executive and advisory oversight mechanisms in place to oversee Secure Flight. As we reported in March 2005, the DHS Investment Review Board (IRB)—designed to review certain programs at key phases of development to help ensure they meet mission needs at expected levels of costs and risks—reviewed the TVP from which Secure Flight will operate, in January 2005.[18] As a result of this review, the board withheld approval for the TVP 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 (cost, schedule, and performance parameters) had been completed. Since that time, TSA has not yet addressed these conditions and has not obtained approval from the IRB to proceed into production. DHS officials stated that an IRB review is scheduled to be held in March 2006—14 months after the IRB last met to examine Secure Flight—to review Secure Flight and other people-screening programs, including international prescreening conducted by CBP. Specifically, the board will review the acquisition strategy and progress for each program, focusing, in part, on areas of potential duplication. According to TSA officials, the agency intends to establish a new program cost, schedule, and capability baseline for Secure Flight, which will be provided to the IRB for review.

DHS's Data Privacy and Integrity Advisory Committee also reviewed Secure Flight during the last year.[19] Committee members have diverse expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the nonprofit sector. In December 2005, the committee issued five recommendations on key aspects of the program, including recommendations designed to minimize data collection and provide an effective redress mechanism to passengers who believe they have been incorrectly identified for additional security scrutiny. TSA officials stated that they are considering

[18] The DHS Investment Review Board also reviewed the CAPPS II program in October 2003 and authorized the program to proceed with the system's development.

[19] The committee was established under the authority of the Homeland Security Act, P.L. 107-296, in accordance with the provisions of the Federal Advisory Committee Act (5 U.S.C. App.2). At the first meeting of the committee, in April 2005, Secure Flight was recommended as a program for examination for numerous reasons, including the number of citizens affected by the program, weaknesses in the program's redress system identified by us in our March 2005 report, and the program's potential use as a model for other related DHS efforts.

the advisory committees' findings and recommendations as part of their rebaselining efforts.

In September 2004, TSA appointed an independent working group within the Aviation Security Advisory Committee,[20] composed of government privacy and security experts, to review Secure Flight. The working group issued a report in September 2005 that concluded, among other things, 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. The group attributed this omission to the lack of a program-level policy document issued by a senior executive, which would clearly state program goals. The working group also questioned Secure Flight's oversight structure and stated that it should focus on the effectiveness of privacy aspects of the program and, in doing so, consider oversight regimes for federal law enforcement and U.S. intelligence activities.

In addition to oversight reviews initiated by DHS and TSA, the DOJ-OIG issued a report in August 2005 reviewing TSC's role in supporting Secure Flight.[21] In its report, the DOJ-OIG reported that TSC faced several key factors that were unknown with respect to supporting Secure Flight, including when the program will begin, the volume of inquiries it will receive, the number of TSC resources required to respond to these inquiries, and the quality of the data it will have to analyze. In light of these findings, the DOJ-OIG report recommended that, among other things, TSC better prepare itself for future needs related to Secure Flight by strengthening its budgeting and staffing processes and by improving coordination with TSA on data exchange standards. In June 2005, a DOJ-OIG report recommended that TSC conduct a record-by-record review of the TSDB to improve overall data quality and integrity. TSC agreed with all recommendations made.[22]

[20] The Aviation Security Advisory Committee, now within DHS, was formed in 1989 to provide advice on a variety of aviation security issues.

[21] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, August 2005. Congress requested that the DOJ-OIG evaluate TSC's plans to support Secure Flight to report these findings to the House and Senate Appropriations Committees.

[22] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center*, June 2005.

TSA Has Made Progress in Coordinating with Critical Stakeholders but More Work Remains

TSA has drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and has begun coordinating with CBP and TSC on Secure Flight requirements and broader issues of integration and interoperability between Secure Flight and other people-screening programs. However, TSA has not yet provided information and technical requirements that all stakeholders need to finalize their plans to support the program's operations, and to adequately plan for the resources needed to do so.

TSA Has Begun Collaborating with Key Stakeholders, but Their Participation Will Be Limited Until System Requirements Have Been Finalized

As we reported in March 2005, key federal and commercial stakeholders—CBP, TSC, and commercial air carriers—will play a critical role in the collection and transmission of data needed for Secure Flight to operate successfully. Accordingly, TSA will need to ensure that requirements for each stakeholder are determined. For instance, TSA will need to define how air carriers are to connect to CBP and what passenger data formats and structures will be used. Although more remains to be done, TSA has worked to communicate and coordinate requirements with stakeholders. For example, TSA has maintained weekly communications with CBP and TSC regarding their roles and responsibilities related to Secure Flight operations.

TSA has also begun to address air carriers' questions about forthcoming Secure Flight requirements. For example, TSA Officials have produced draft air carrier guidance, known as the Secure Flight Data Transmission Plan Guidance (DTPG).[23] The final DTPG is to include guidance to air carriers addressing the following areas: Secure Flight's mission overview and objectives, project planning phases, aircraft operator operations and airport procedures, technical data requirements, aircraft operator application development, Secure Flight operations, and system maintenance and support. According to TSA officials, air carriers have received copies of a partial draft DTPG, and some air carriers have submitted feedback to Secure Flight's Airline Implementation and Operations Team that TSA says it is working to address.

[23] The current draft of the DTPG also includes several appendices that provide additional, detailed program information to airlines, including an Interface Control Document containing detailed technical information such as message content and screen layout, a high-level technical plan for implementing various components of Secure Flight, detailed programming specifications for message timing and instructions for various passenger vetting scenarios, a recommendation that the airline industry develop an industry standard method for communicating Full Name (FN) and Date of Birth (DOB), and the system operational test plans.

In addition to drafting guidance, TSA has conducted preliminary network connectivity testing between TSA and federal stakeholders. For example, messages have been transmitted from CBP to TSA and back. However, such tests included only dummy data. According to CBP officials, no real-time passenger data have been used in this testing, and system stress testing has not yet been conducted.[24] Without real-time passenger data, the official said, CBP cannot estimate total capacity or conduct stress testing to ensure the system operates effectively. Further, according to a TSC official, testing has been conducted to show that a data exchange between the TSC and TSA is functioning, but the system has not been stress-tested to determine if it can handle the volume of data traffic that will be required to operate Secure Flight. According to this official, TSA has not specified what these data volume requirements will be. TSA officials acknowledged that they have not yet made this determination and stated that they will not be able to do so until they (1) issue the rule, and (2) have received the air carrier plans for participating in Secure Flight based on requirements identified in the rule.

Although CBP, TSC, and air carrier officials we interviewed 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 cannot proceed with establishing connectivity with all air carriers until DHS publishes the rule—the regulation that will specify what type of information is to be provided for Secure Flight—and the air carriers provide their plans for providing this information. Similarly, a TSC official stated that TSC cannot make key decisions on how to support Secure Flight until TSA provides estimates of the volume of potential name matches that TSC will be required to screen, as identified above. The TSC official stated that without this information, TSC cannot make decisions about required resources, such as personnel needed to operate its call center.[25] As we reported in March 2005, air carriers also expressed concerns regarding the uncertainty of the Secure Flight system and data requirements, and the impact these requirements may have on the airline industry and traveling public. Air carriers will not be able to begin to modify their passenger data

[24] Stress testing refers to measuring a system's performance and availability in times of particularly heavy (i.e., peak) load.

[25] According to the DOJ-OIG, when Secure Flight becomes operational, TSC anticipates a significantly greater operational workload as a result of the program and an increased need for staff, space, and funding.

systems to record the data attributes—such as full name and date of birth, which Secure Flight will use to conduct name matching—until TSA determines and communicates which specific data attributes are to be used.

Oversight groups that have reviewed Secure Flight agreed that additional work was needed to improve the flow of information to, and coordination with, program stakeholders. In its December 2005 report on Secure Flight, the DHS Data Privacy and Integrity Advisory Committee stated that TSA needs to be clear with air carriers about what information it needs now and what information it may consider requesting in the future, to enable air carriers to avoid sequential revisions of data-handling systems. Also, in September 2005, the Aviation Security Advisory Committee working group expressed concerns about the lack of clarity regarding how Secure Flight will interact with other screening programs.

Further, in its August 2005 audit of TSC's support of Secure Flight, the DOJ-OIG reported that TSC officials believed that their ability to prepare for the implementation of Secure Flight has been hampered by TSA's failure to make, communicate, and comply with key program and policy decisions in a timely manner, such as the launch date and volume of screening to be conducted during initial implementation. In addition, the report noted that because TSA is unsure about how many air carriers will participate in the initial phase of the program, neither TSA nor TSC can know how many passenger records will be screened, and cannot project the number of watch list hits that will be forwarded to the TSC for action. Finally, the DOJ-OIG report concluded that the shifting of critical milestones—including TSA's schedule slippages over the past year—has affected TSC's ability to adequately plan for its role in Secure Flight.

Despite TSA's outreach efforts, stakeholder participation in Secure Flight is dependent on TSA's effort to complete its definition of requirements and describe these in the rule. Because TSA has not fully defined system requirements, key stakeholders have not been able to fully plan for or make needed adjustments to their systems. In our March 2005 report, we recommended that TSA develop a plan for establishing connectivity among the air carriers, CBP, and TSC to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations. Although TSA has continued to coordinate with these key stakeholders, at present the agency has still not completed the plans and agreements necessary to ensure the effective support of Secure Flight.

Ongoing Coordination of Prescreening and Name-Matching Initiatives Can Impact How Secure Flight Is Implemented

In January 2006, TSA officials stated that they are in the early stages of coordinating with CBP on broader issues of integration and interoperability related to other people-screening programs. These broader coordination efforts, which are focused on minimizing duplicative efforts that may exist between the agencies that screen individuals using watch list data and achieving synergies and efficiencies, are important because they may affect how Secure Flight will operate initially and in the future. Specifically, 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 prescreening function through coordinated information connections and avoid unnecessary duplication of communications, programming, and information requirements.[26]

In response to air carrier concerns, and the initiatives of DHS to minimize duplicative efforts, officials from both CBP and TSA explained that they are beginning to work together to ensure that air carriers have a single interface with the government for prescreening both domestic and international passengers. TSA and CBP officials further stated that they will try to use CBP's network to transmit domestic and international passenger data to and from the air carriers, thus providing the air carriers with a single interface for sending and receiving information.[27] TSA and CBP officials also stated that air carriers should receive a common notification about whether a passenger—domestic or international—requires normal processing, additional screening, or is not permitted to board a plane. However, according to these officials, TSA and CBP have not yet resolved other system differences—such as the fact that their prescreening systems use different passenger data elements, documentation,[28] and name matching technologies—that could lead to conflicting notifications that would instruct air carriers to handle a

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

[27] CBP and TSA officials stated they will use this same network to transmit data for their respective international and domestic prescreening efforts. Different addresses on the passenger information will ensure that TSA and CBP data are routed to the appropriate handling agencies for screening.

[28] For international prescreening, name-matching is conducted using data elements from a passport, whereas passports are not required for domestic flights.

passenger differently for an international than for a domestic flight. Both TSA and CBP officials agreed that additional coordination efforts are needed to resolve these differences, and stated that they plan to work closely together in developing a prescreening capability for both domestic and international passengers.[29] Decisions made as a result of further coordination could result in changes to the way that Secure Flight is implemented.

In addition to coordinating with CBP on international prescreening, TSA faces additional coordination challenges working with TSC. Specifically, according to TSC officials, TSC has an initiative under way to, among other things, better safeguard watch list data. Currently, TSC exports watch list data to other federal agencies, such as TSA and the State Department, for use in these agencies' screening efforts or processes for examining documents and records related to terrorism. However, TSC is currently developing a new system whereby watch list data would not be exported, but rather would be maintained by TSC. This system, called Query, is to serve as a common shared service that will allow agencies to directly search the TSDB using TSC's name matching technology for their own purposes. TSC has conducted limited testing of the system. If TSC chooses to use Query, TSA will be required to modify the system architecture for Secure Flight in order to accommodate the new system. According to a TSC official, this effort could be costly. While TSA acknowledged in its draft concept of operations plan in June 2005 that Secure Flight would need to be modified to accommodate TSC's Query "as necessary," the agency has not made adjustments to its system requirements or conducted a cost analysis of expected impacts on the Secure Flight program. Rather, TSA has decided that it will continue developing the Secure Flight application, which includes TSA's name-matching technologies. Thus, TSC will need to export watch list data to TSA to support Secure Flight, once it becomes operational.

[29] We currently have an on-going review of CBP's international prescreening process, including assessing the current process for conducting international passenger prescreening and reviewing the benefits and challenges of implementing additional or enhanced international prescreening strategies.

Key Factors That Will Influence the Effectiveness of Secure Flight Have Not Been Finalized or Resolved

Several activities are under way, or are to be decided, that will affect Secure Flight's effectiveness, including how operational testing is conducted, and how data requirements and data accuracy are determined. TSA has been testing and evaluating name-matching technologies for determining what type of passenger data will be needed to match against the TSDB. These tests have been conducted thus far in a controlled, rather than real-world environment, using historical data, and additional testing is needed. In addition, TSA has not made key decisions regarding how the name-matching technologies to be used by Secure Flight will operate or which data will be used to conduct name matching. While TSA is not responsible for ensuring the accuracy of passenger data, the agency must nonetheless advise stakeholders on data accuracy and quality requirements. Another 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 passengers who use false identifying information. Secure Flight is neither intended to nor designed to address these vulnerabilities.

Tests of Name-Matching Capability Are Under Way, but Full System Testing Has Not Yet Been Conducted

TSA has tested—and continues to test—the effectiveness of one aspect of the Secure Flight system, namely name-matching technologies. These name-matching tests will help TSA determine what passenger data will be needed for the system to match most effectively passenger records with information contained in the TSDB. These tests are critical to defining data requirements and making decisions about how to configure the name-matching technologies. Additional tests will need to be conducted in an operational, real-world environment to fully understand how to configure the system effectively. This is because the name-matching tests conducted to date were conducted in a controlled, rather than real-world, environment—that is, under controlled, or simulated, conditions. For example, TSA used historic air carrier passenger data from June 2004 and historic and simulated watch list data to test the functionality and effectiveness of Secure Flight's name-matching technologies that match air carrier passenger records with potential terrorists in the TSDB.

Additional testing beyond name-matching also needs to be conducted, after TSA rebaselines its program, defines system requirements, and begins adhering to its SDLC. For example, stress and operational testing[30] would help determine whether Secure Flight can process the volume of data expected and operate as intended in an operational environment. As we reported in March 2005, TSA had planned to conduct a series of operational tests consisting of increasingly larger increments of the system's functionality until the complete system was tested. These tests were to begin in June 2005. However, due to program delays, TSA has not yet conducted this end-to-end testing needed to verify that the entire system, including any interfaces with external systems, functions as intended in an operational environment. TSA also has not yet conducted the stress testing needed to measure the system's performance and availability in times of particularly heavy (i.e., peak) loads. Recently, TSA documented its overall strategy for conducting these tests and developed draft test plans. TSA officials stated that information about its plans for future testing will be included in its rebaselined program plan. Until this testing is complete, it will not be possible to determine whether Secure Flight will function as intended in an operational environment.

Key Policy Decisions That Will Impact System Effectiveness Have Not Been Made

Key policy decisions that will influence the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny have not yet been made. These policy decisions include (1) determining the passenger information that air carriers will be required to collect and provide for vetting, (2) the name-matching technologies that will be used to vet passenger data against data contained in the TSDB, and (3) the thresholds that will be set to determine when a passenger will be identified as a potential match against the TSDB. These three decisions, discussed below, are all critical to ensuring that Secure Flight identifies potential terrorist threats as effectively as possible while minimizing the number of potential matches that will require further review by TSA and TSC analysts.

(1) *Determining the passenger information that air carriers will be required to collect and provide for vetting*: TSA needs 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.

[30] Whereas stress testing is used to determine the maximum capacity of the system, operational testing is used to ensure that the system operates as intended, including the people and the information technology systems operating together in their expected environments.

Using too many data attributes can increase the difficulty of matching, since the risk of errors or mismatches increases. Using too few attributes can create an unnecessarily high number of incorrect matches due to, among other things, the difficulty of differentiating among similar common names without using further information. Initial TSA test results have shown that the use of name and date of birth alone might not be sufficient for decreasing the number of false positives—that is, passengers inappropriately matched against data contained in the TSDB.

(2) *Selecting name-matching technologies used to vet passenger names against the TSDB*: TSA must determine what type or combination of name-matching technologies to acquire and implement for Secure Flight, as these different technologies have different capabilities. For example, TSA's PNR testing showed that some name-matching technologies are more capable than others at detecting significant name modifications, which allows for the matching of two names that contain some variation. Detecting variation is important because passengers may intentionally make alterations to their names in an attempt to conceal their identity. Also, unintentional variations can result from different translations of nonnative names or data entry errors. For example, some name-matching technologies might correctly discriminate between "John Smith" and "John Smythe," others may not. However, name matching technologies that are best at detecting name variations may also increase the number of potential matches that will have to be further reviewed, which could be offset using a combination of name matching technologies. TSA officials stated in November 2005 that it planned to continuously evaluate the best name-matching technologies or combination of technologies to enhance the system in future iterations. TSA officials recently stated that they had made, but not yet documented, an initial determination regarding the name-matching technologies that will be used for Secure Flight and that they plan to conduct continuous reviews of the name-matching technologies to address circumstances as they arise.

(3) *Selecting thresholds for determining when a possible name match has occurred*: TSA has discretion to determine what constitutes a possible match between a passenger's data and a TSDB record.[31] For each name that is matched, the name-matching tool will assign a numeric score that

[31] The name matching process depends on the level of false positive and false negative matches deemed acceptable. False negatives are passengers incorrectly not matched to a watch list.

indicates the strength of the potential match.[32] For example, a score of 95 out of 100 would indicate a more likely match than a score of 85. If TSA were to set the threshold too high, many names may be cleared and relatively few flagged as possible matches—that is, there is a possibility that terrorists' names may not be matched. Conversely, if the threshold were set too low, passengers may be flagged unnecessarily, and relatively few cleared through the automated process. As an example of the importance of setting thresholds, during one of the PNR tests conducted, TSA set the name-matching threshold at 80, which resulted in over 60 percent of passengers requiring manual review. Alternatively, when TSA set the threshold at 95, less than 5 percent of the same group of passenger records were identified as requiring further review. With about 1.8 million passengers traveling domestically per day, having a threshold that is too low could produce an unmanageable number of matches—possibly leading to passenger delays—while setting the threshold too high could result in the system missing potential terrorists. Although TSA will not decide how the thresholds should be set until it conducts additional evaluations, it has indicated that the threshold might be adjusted to reflect changes in the terrorist threat level. This would result in Secure Flight flagging more names for potential manual review in order to ensure greater scrutiny in response to changing conditions.

TSA plans to finalize decisions on these factors as system development progresses. However, until these decisions are made, requirements will remain unsettled and key stakeholders—in particular air carriers—will not have the information they need to assess and plan for changes to their systems necessary for interfacing with Secure Flight. Air carriers and reservation companies will also not know which additional data attributes they may be required to collect from passengers, to support Secure Flight operations, as reservations are made. These decisions will also directly influence the number of analysts that TSA and TSC will need to manually review potential matches to the TSDB. Accordingly, stakeholders have expressed concern that they have not been provided information about what these decisions are. They stated that they are awaiting additional information from TSA in order to move forward with their plans to interface with and support Secure Flight.

[32] The score is based, in part, on how much weight is given to, say, name or date of birth relative to each other.

Efforts to Improve Data Quality and Accuracy Are Under Way, but Additional Work Remains

Two additional factors that will impact the effectiveness of Secure Flight are (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, in order to minimize inconveniencing passengers. According to TSA and TSC officials, the data attributes that Secure Flight will require for name matching need to be included in both the passenger data and the TSDB in order for the automated system to effectively match names between the two lists. As we reported in March 2005, while the completeness and accuracy of data contained in the TSDB can never be certain—given the varying quality of intelligence information gathered, and changes in this information over time—TSC has established some processes to help ensure the quality of these data. However, the DOJ-OIG, in its June 2005 review of TSC,[33] found that that the TSC could not ensure that the information contained in its databases was complete or accurate.[34] According to a TSC official, since the time of the DOJ-OIG review, TSC has taken several steps to improve the quality of TSDB records, including conducting a record-by-record review, updating procedures for a daily review of each new or modified record, and using automated rules to check the completeness of records received from other agencies.[35] According to this official, TSA and TSC plan to enter into a letter of agreement that will describe the TSDB data elements that TSC will produce for TSA, among other things, to be used for Secure Flight. However, these data requirements have not yet been determined.

In order to obtain accurate and complete passenger data from air carriers, TSA plans to describe the required data attributes that must be contained in passenger data provided to TSA in the forthcoming rule. TSA also plans to issue a final and complete DTPG to specify the data formats and other transmission requirements. However, the accuracy and completeness of the information contained in the passenger data record will still be dependent on the air carriers' reservations systems and passengers, and

[33] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center*, June 2005. According to the DOJ Office of the Inspector General's report, some errors in the TSDB might be corrected by a manual review conducted by intelligence analysts and a redress process.

[34] We have an ongoing review of the reasons misidentifications occur using TSDB data, and the efforts by the TSC and other agencies to reduce these errors.

[35] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, August 2005.

the air carriers' modifications of their systems for transmitting the data in the proper format. These steps are not trivial, as indicated by the June 2004 historical passenger data provided by the air carriers for TSA's name-matching tests. For these tests, many passenger data records submitted by air carriers were found to be inaccurate or incomplete, creating problems during the automated name-matching process. For example, some passenger data included invalid characters or prefixes, such as "Mr." and "Mrs.," in the name fields. Other inaccuracies included invalid characters or prefixes, spelling errors, and inverted birth date information. Additionally, some of the records had omitted or incomplete data elements necessary for performing the automated match or were in an unusable format.

In a related effort to address accuracy, TSA and TSC plan to work together 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 will use intelligence analysts during the actual matching of passenger data to data contained in the TSDB to increase the accuracy of data matches. As indicated in figure 1, when TSA's name-matching technologies indicate a possible match, TSA analysts are to manually review all of the passenger data and other information to determine if the passenger can be ruled out as a match to the TSDB. If a TSA analyst cannot rule out a possible match, the record will be forwarded to a TSC analyst to conduct a further review using additional information. According to a TSC official, TSA and TSC analysts participated in a tabletop exercises to test the consistency of their respective manual reviews, and found that the matching logic used by both groups of analysts was consistent. This official stated that TSA and TSC also tested their operational procedures, and found gaps in their procedures that are now being addressed. According to this official, TSA and TSC plan to conduct additional joint exercises. Completing these exercises will be important to further understanding the effectiveness of using intelligence analysts to clear misidentified passengers during Secure Flight operations.

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

Another factor that could affect Secure Flight's effectiveness in identifying known or suspected terrorists is the system's inability to identify passengers who falsify their identifying information or who commit identity theft.[36] TSA Officials stated that the program is not intended to or designed to protect against the use of falsified identities or to detect identity theft. However, TSA officials stated that the use of commercial data during the name-matching process may help identify situations in which a passenger submits fictitious information such as a false address. In the spring of 2005, a TSA contractor tested the use of commercial data composed of personally identifiable information (such as name and address) to determine, among other things, if such data could be used to increase Secure Flight's effectiveness in identifying false or stolen identities. However, according to the DHS Data Privacy and Integrity Advisory Committee report, testing performed to date does not provide a reasonable case for utilizing commercial data as part of Secure Flight. TSA officials are not currently pursuing the use of commercial data to support Secure Flight because the fiscal year 2006 DHS appropriations act prohibits TSA from using data or databases obtained from or that remain under the control of a non-federal entity,[37] effectively terminating this type of testing for the duration of fiscal year 2006.[38] Further, TSA officials stated that incorporating biometrics—technologies that can automate the identification of people by one or more of their distinct physical or behavioral characteristics—is not currently envisioned for Secure Flight. As noted in our previous work, biometric technologies, such as fingerprint recognition, are being used in other TSA screening programs.[39] Moreover, the current prescreening process of matching passenger names against no-fly and selectee lists implemented by air carriers also does not protect against identity theft or the use of fictitious identities.

[36] Falsifying identifying information involves passenger attempted 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). This is sometimes referred to as identity fraud.

[37] The Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109-90, § 518 (e), 119 Stat. 2064, 2085 (2005).

[38] This prohibition on the use of appropriated funds does not apply to passenger name record data obtained from air carriers.

[39] GAO, *Aviation Security: Challenges in Using Biometric Technologies*, GAO-04-785T (Washington, D.C.: May 19, 2004).

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 impact their rights. However, TSA, as part of its requirements development process, has not yet clearly identified the privacy impacts of the planned system or the full actions it plans to take to mitigate them. Nor has the agency completed its assessment of the potential impact on passenger privacy of the system in an operational environment or defined its redress process for Secure Flight because, in part, the operational plans and system requirements for Secure Flight have not been finalized. TSA officials stated that they are in the process of reviewing new privacy notices that will be issued in conjunction with a forthcoming rule making prior to proceeding with its initial operating capability, and that these notices will also address certain aspects of Secure Flight's redress process. Until TSA finalizes system requirements and notices, however, privacy protections and impacts cannot be assessed.

Privacy Cannot Be Fully Assessed Because System Development Documentation Does Not Fully Address Privacy Requirements

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.[40] While TSA has reiterated its commitment to meet the requirements of the Privacy Act and the Fair Information Practices, it is not yet evident how this will be accomplished.[41] To begin with, TSA has not decided what data attributes from the PNR it plans to collect, or how such data will be provided by airlines, through CBP, to TSA. Further, according to TSA officials, the agency is in the process of developing but has not issued the system of records notice, which is required by the Privacy Act,[42] or the privacy impact assessment, which is required by the E-Government Act,[43] that would describe how TSA considered privacy in

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

[41] Also, in its mandate regarding Secure Flight, Congress asked that GAO review whether there are any specific privacy concerns with the technological architecture of the Secure Flight system.

[42] 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. See § 552a(e)(4).

[43] 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.

the development of the system and how it will protect passenger data once the system becomes operational.

Moreover, privacy requirements were not incorporated into the Secure Flight system development process in such a way that would explain whether personal information will be collected and maintained in the system in a manner that complies with statutory requirements and TSA's SDLC guidance. One requirement of the privacy impact assessment is that privacy be addressed in the systems development documentation. In addition, TSA's SDLC guidance acknowledges that privacy protections should be planned for and carried out as part of the system development process. In our review of Secure Flight's system requirements, we found that privacy concerns were broadly addressed in Secure Flight's functional requirements, but had not been translated into specific system requirements. For example, the functional requirements stated that the Privacy Act must be considered in the development of the system, but the system requirements documents do not reflect how privacy protections will be supported by the system. Rather, system requirements documents state that privacy requirements are "yet to be finalized." TSA's Privacy Officer stated that she has been collaborating with the system development team, but this is not evident in the documents we reviewed.

Without taking steps to ensure that privacy protections are built into the system requirements, TSA cannot be assured that it will be in compliance with the Privacy Act once operational, and it runs the risk of repeating problems it experienced last spring. We reported in July 2005 that TSA's initially issued privacy notices for the Secure Flight data-processing tests did not meet Privacy Act requirements because personal information was used in testing in ways that the agency had not disclosed to the public.[44] We explained that in its fall 2004 notices, TSA had informed the public of its plans to use personal information during Secure Flight testing, including the use of commercial data in a limited manner. However, these initial notices did not fully describe how personal information would be collected, used, and stored for commercial data testing as it was carried out. As a result, individuals were not fully informed that their personal information was being collected and used, nor did they have the opportunity to comment on this or become informed on how they might

[44] GAO, *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).

exercise their rights of access to their information. Although TSA did not fully disclose its use of personal information prior to beginning Secure Flight commercial data testing, the agency issued revised privacy notices in June 2005 to more fully disclose the nature of the commercial tests and address the issues disclosed by us.

As we reported in March 2005, until TSA fully defines its operational plans for Secure Flight 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. At that time, we recommended that TSA finalize privacy policies and issue associated documentation prior to Secure Flight achieving initial operating capability. TSA acknowledged that it needs to publish new privacy notices to cover the collection, use, and storage of personal data for Secure Flight's initial and full operating capability, before beginning operational testing. TSA officials stated that these privacy notices are currently being reviewed by TSA and DHS and will be released in conjunction with the forthcoming rulemaking.

TSA Has Not Determined Secure Flight's Redress Process

Congress mandates 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.[45] TSA currently has a process in place that allows passengers who experience delays, under the current process run 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 that in the future the passenger may still experience delays.[46] Recently, TSA has automated the

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

[46] TSA's Office of Transportation Security Redress manages redress for the current watch list matching process conducted by the air carriers. Currently OTSR is developing an agency-wide policy for redress and has interviewed TSA Officials as part of this effort, but found that Secure Flight requirements were not sufficiently defined for use in drafting the new policy. TSA officials stated that they are continuing to discuss the Secure Flight redress process with OSTR.

cleared list process, enabling the agency to further mitigate inconvenience to travelers on the cleared list.

The Intelligence Reform and Terrorism Prevention Act, enacted in December 2004, directs TSA to include certain elements in its Secure Flight redress policy.[47] Specifically, it requires the establishment of a timely and fair process for individuals identified as a threat to appeal the determination to TSA and correct any erroneous information.[48] It further requires that TSA establish a method for maintaining a record of air passengers who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers, this record must contain information determined by TSA to authenticate the identity of such a passenger. In January 2006, TSA officials stated that no final decisions have been made regarding how TSA will address the relevant requirements for redress found in the Intelligence Reform and Terrorism Prevention Act requirements. However, OTSR officials stated that a cleared list will be part of the process. The June 2005 concept of operations describes a process where individuals that are frequently misidentified as being on the TSDB and TSA selectee list can request to be placed on a list of individuals who have been cleared.

In our March 2005 report, we recommended that TSA finalize its Secure Flight redress policies and procedures prior to achieving its initial operating capability. Information concerning aspects of the redress process will be published before operational tests or full implementation of the Secure Flight process, and will be contained within the privacy notices that TSA officials stated will be released in conjunction with the forthcoming rulemaking. Moving forward, TSA has assigned a manager to serve as liaison with DHS on privacy and redress issues.

[47] See Pub. L. No. 108-458, § 4012(a) (codified at 49 U.S.C. § 44903(j)(2)(C), (G)).

[48] This requirement generally addresses principles from both the Privacy Act—that individuals be able to access and correct their personal information—and the Fair Information Practice of individual participation—that individuals be able to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of such requests. However, Secure Flight's redress system will be challenging for two significant reasons. First, much of the information underlying decisions to add individuals to the TSDB is likely to be classified, and as such will not be accessible to passengers. Second, TSA does not control the content of the TSDB that it intends to use as the primary input in making screening decisions.

Concluding Observations

TSA has continued its development and testing of Secure Flight, but has made limited progress in addressing longstanding issues related to system development and testing, program management, and privacy and redress protections. To make and demonstrate progress on any large-scale information technology program, such as Secure Flight, an agency must first adequately define what program capabilities, such as requirements related to performance, security, privacy, and data content and accuracy, are to be provided. 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; developing life cycle cost estimates and a comprehensive set of critical performance measures; issuing new privacy notices; and putting a redress process in place. Over the past 11 months, TSA has made some progress on all of these areas, including conducting further testing of factors that could influence system effectiveness and corroborating with key stakeholders. However, TSA has not completed any of the actions it had scheduled to accomplish. In particular, TSA has not yet developed complete system requirements or conducted important system testing (including stress testing), fully established security measures, made key decisions that will determine system effectiveness, developed a program management plan and a schedule for accomplishing program goals, or published updated privacy and redress notices. Taken as a whole, this lack of progress indicates that the program has not been effectively managed and is at risk of failure.

While we recognize that TSA faces program uncertainties that can directly impact Secure Flight's development and progress, uncertainty is a component of most programs, and should not be used as a reason for not defining requirements and developing plans and cost estimates, to manage risk. We believe that Secure Flight, like all programs, can utilize best practices to develop such plans to manage program uncertainties.

To its credit, TSA has recently taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program manager with information systems program management credentials. We also support TSA's efforts to rebaseline the program, including defining system requirements and finalizing a program management plan, including the development of schedules and cost estimates, before proceeding with program development. In fact, proceeding with operational testing and completing other key program activities should not be pursued until TSA puts in place a more disciplined life cycle process and defines system requirements. In the absence of this and other program information, such as requirements, capabilities, and benefits, further investment in this program would be difficult to justify.

We are also encouraged that DHS's IRB—the executive decision making authorities—has scheduled a review of Secure Flight and other people-screening programs. Given the potential duplication with CBP's new initiatives for international prescreening, DHS, TSA, and CBP need to assess alternative system solutions that should be factored into Secure Flight's rebaselined program and be the basis for IRB decisions regarding Secure Flight's future. Notwithstanding these efforts, however, much work remains to be accomplished before Secure Flight is positioned to be properly executed so that informed and prudent investment decisions can be made.

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 David Alexander, Amy Bernstein, Mona Nichols Blake, John de Ferrari, Christine Fossett, Brent Helt, Richard Hung, Thomas Lombardi, C. James Madar, Matthew Mohning, David Plocher, Karl Seifert, and William Wadsworth.

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

Legislative mandated issue (number and short title)	Description of mandated issue
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 TSA may appeal such decisions and correct erroneous information contained in CAPPS II or Secure Flight or other follow-on/successor programs.
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.
3. 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.
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.
5. Operational safeguards	TSA has built in sufficient operational safeguards to reduce the opportunities for abuse.
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.
7. Oversight of system use and operation	TSA has adopted policies establishing effective oversight of the use and operation of the system.
8. Privacy concerns	There are no specific privacy concerns with the technological architecture of the system.
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.
10. Life-cycle cost estimates and expenditure plans	Appropriate life-cycle cost estimates, and expenditure and program plans exist.

Source: GAO.

(440422)

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

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-05-356

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.

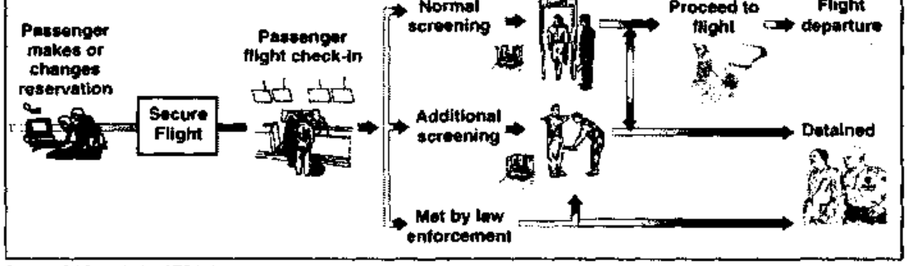
What GAO Found

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).

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.

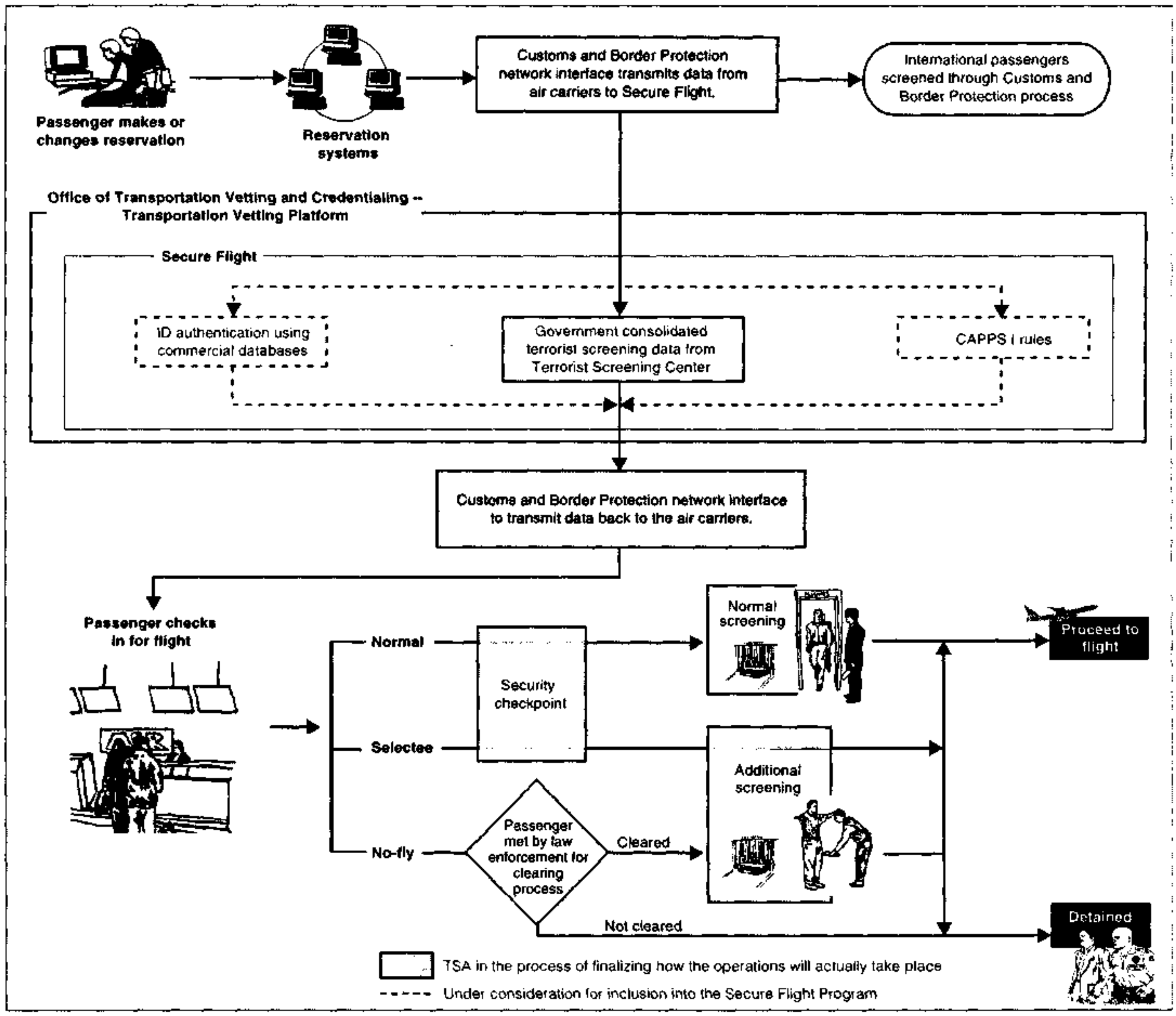
[d] TSA plans to examine whether Secure Flight will use an opt-in list, which could include those passengers participating in TSA's Registered Traveler program.

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
Passenger met by law enforcement for clearing process
Cleared
Not cleared
Normal screening
Additional screening
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.

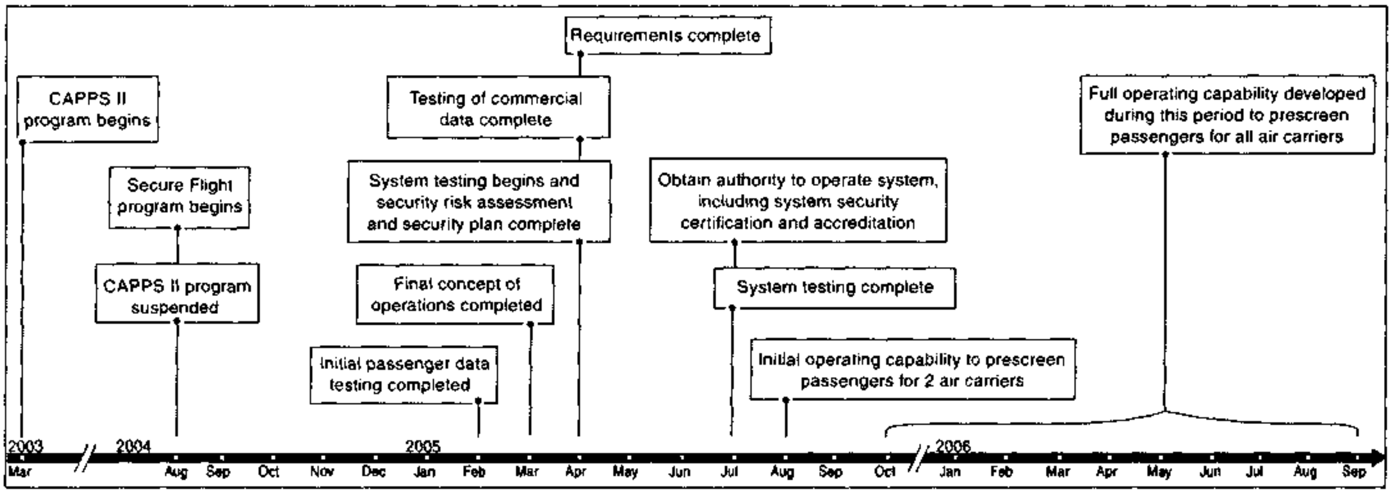
TSA Recently Developed a Comprehensive Schedule, but Key System Documentation and Development Activities Have Not Yet Been Completed

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.

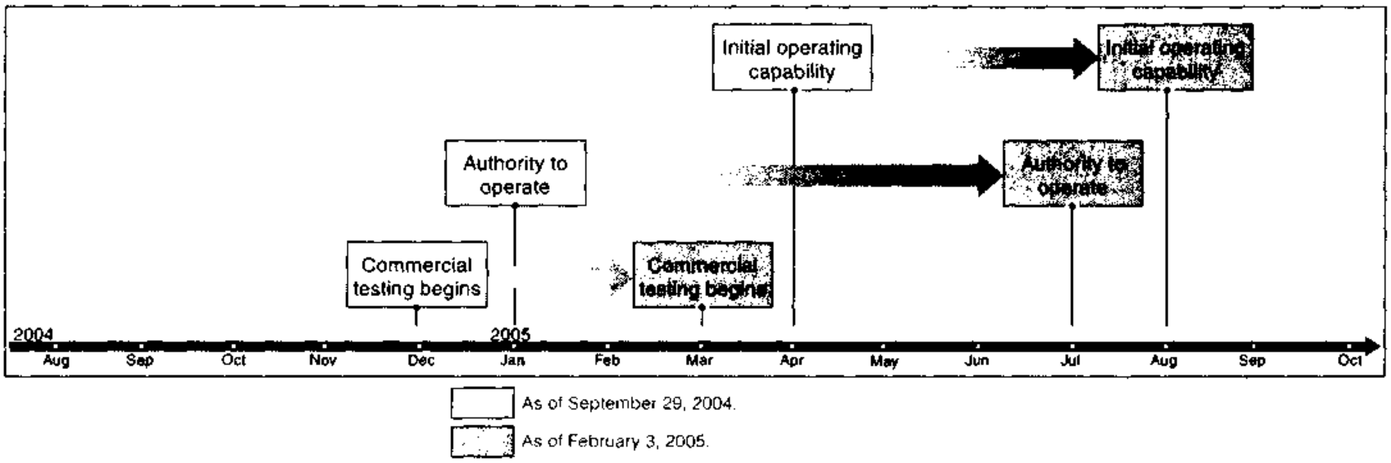
Figure 2: TSA Projected Key Milestones for the Development and Implementation of Secure Flight, as of March 2005



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

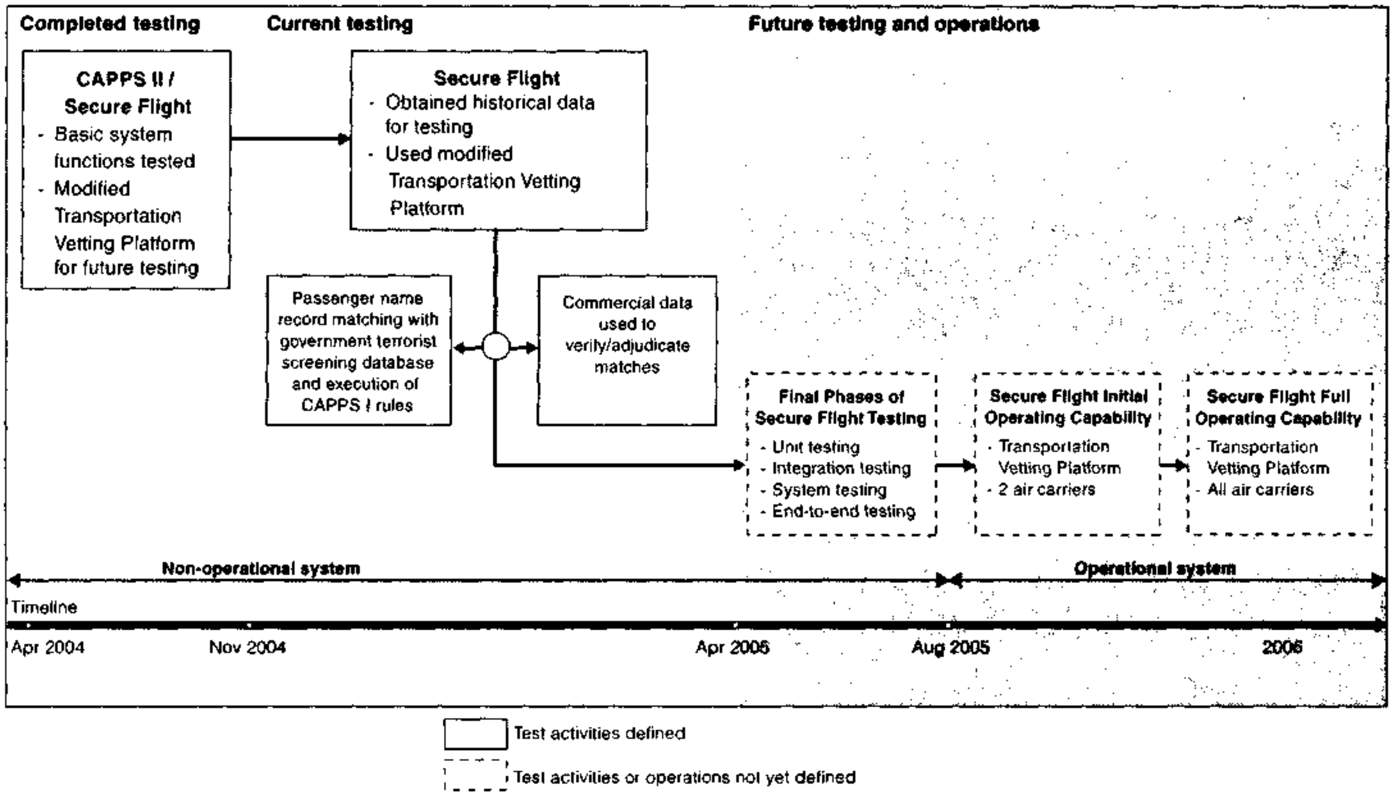


Source: GAO analysis of TSA data.

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.[34] We also found that TSA's acquisition policies and procedures had not been effectively communicated across the agency. Since our review, TSA has

[34] 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

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.

Area of Congressional Interest: Operational Safeguards and Security Measures

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.

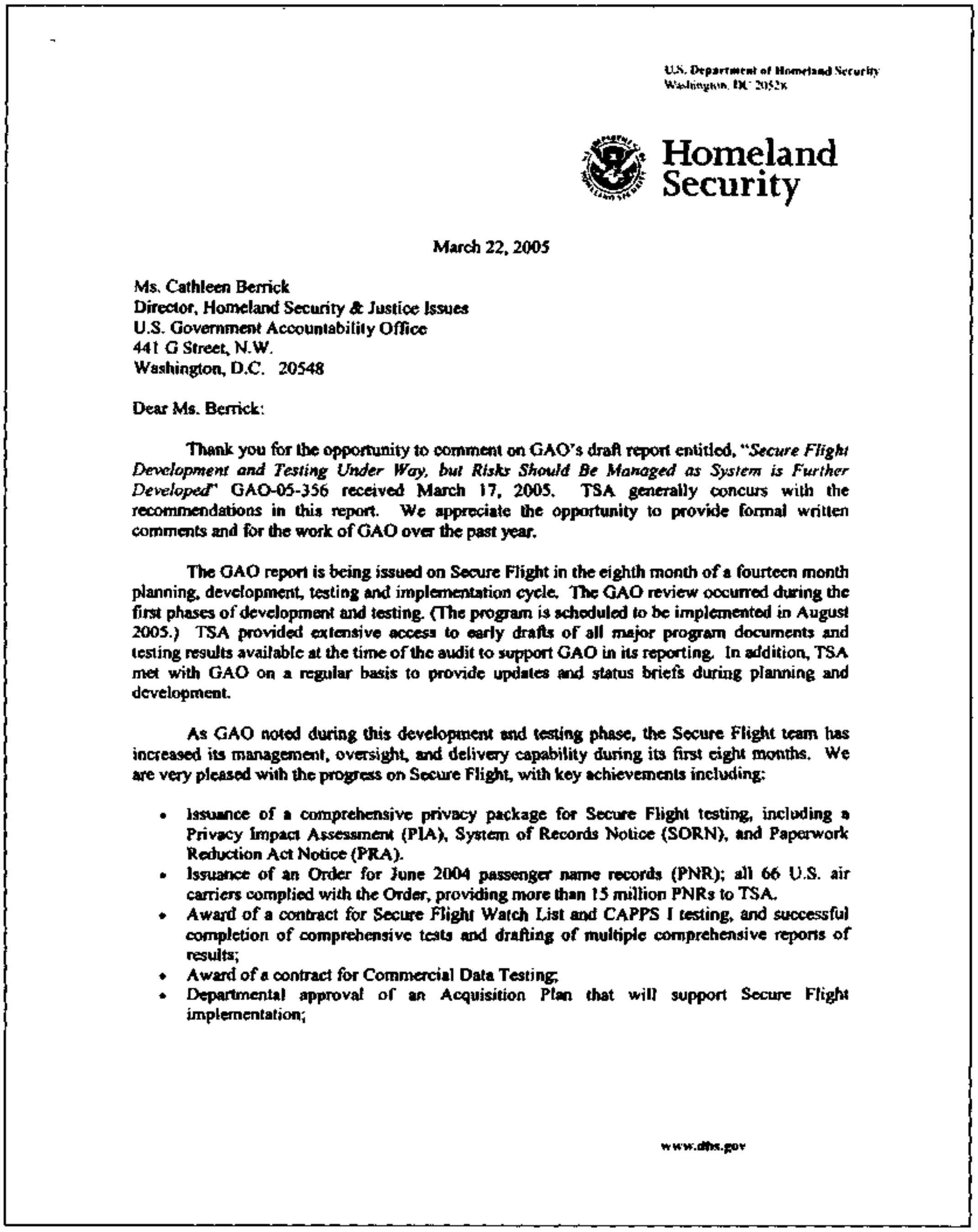
Table 5: Cross-references of Legislatively Mandated Issues to Be Reviewed by GAO with the Sections in this Report

		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			

		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**
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:

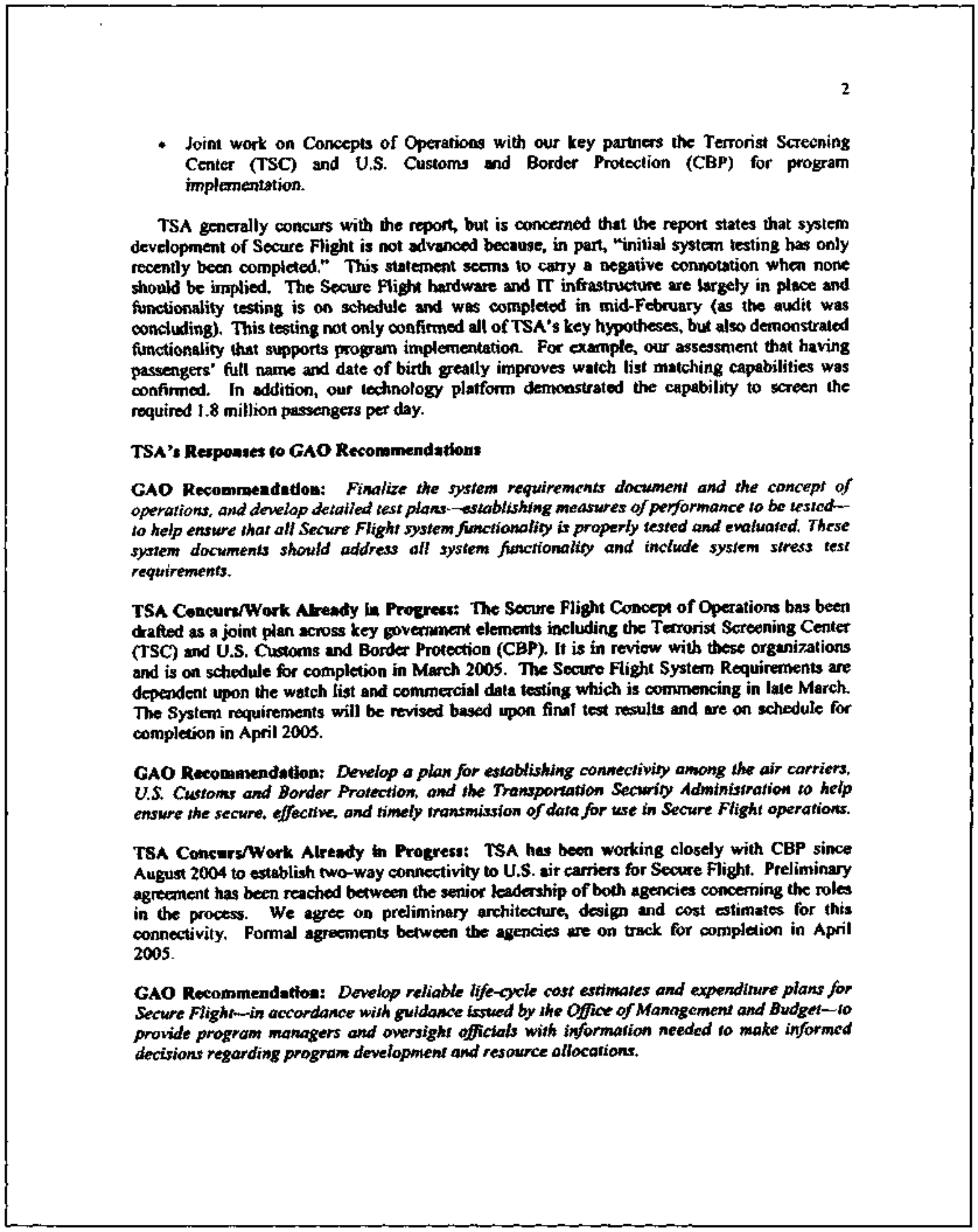
Thank you for the opportunity to comment on GAO's draft report entitled, "*Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed*" GAO-05-356 received March 17, 2005. TSA generally concurs with the recommendations in this report. We appreciate the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

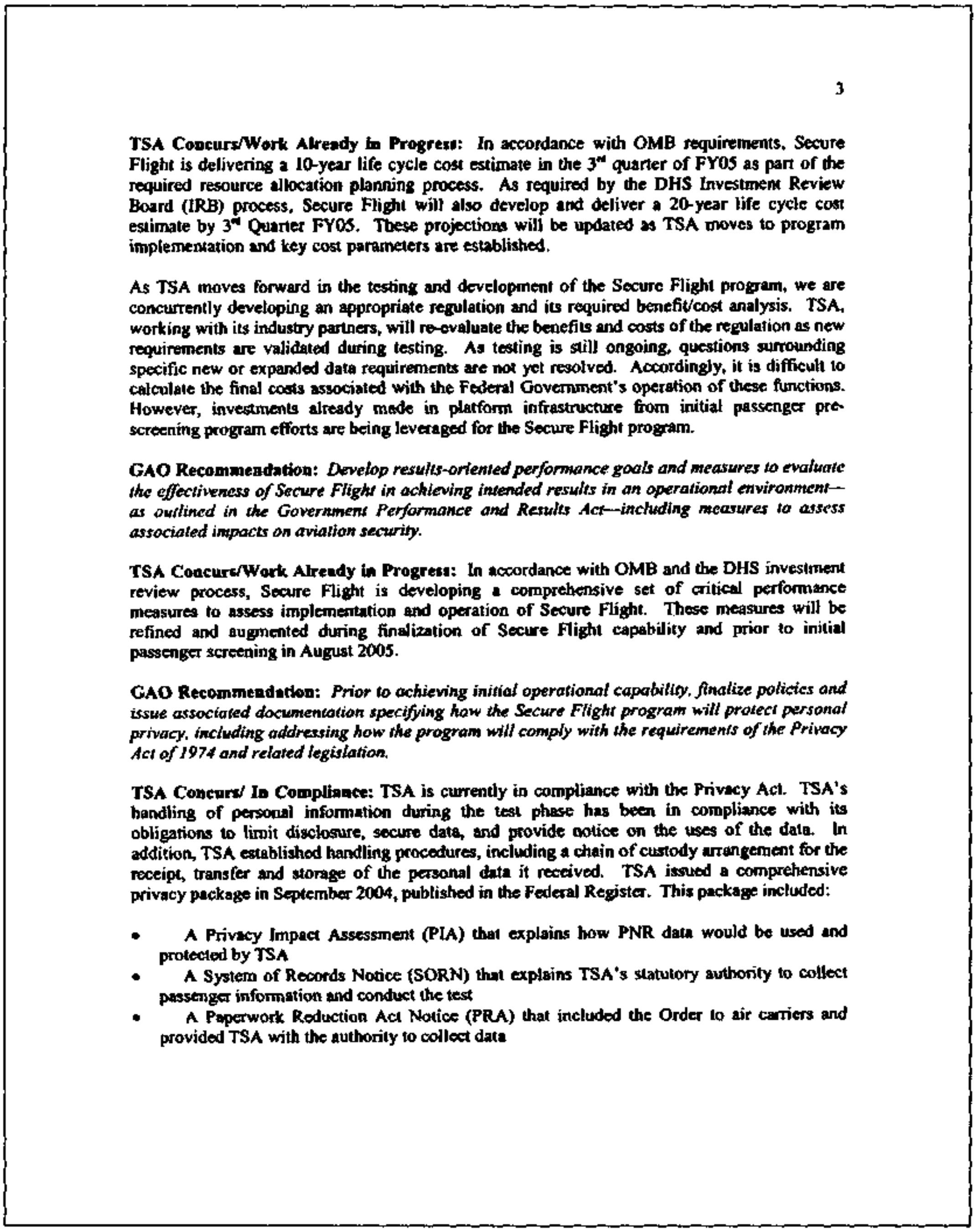
GAO Recommendation: *Finalize the system requirements document and the concept of operations, and develop detailed test plans—establishing measures of performance to be tested—to help ensure that all Secure Flight system functionality is properly tested and evaluated. These system documents should address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

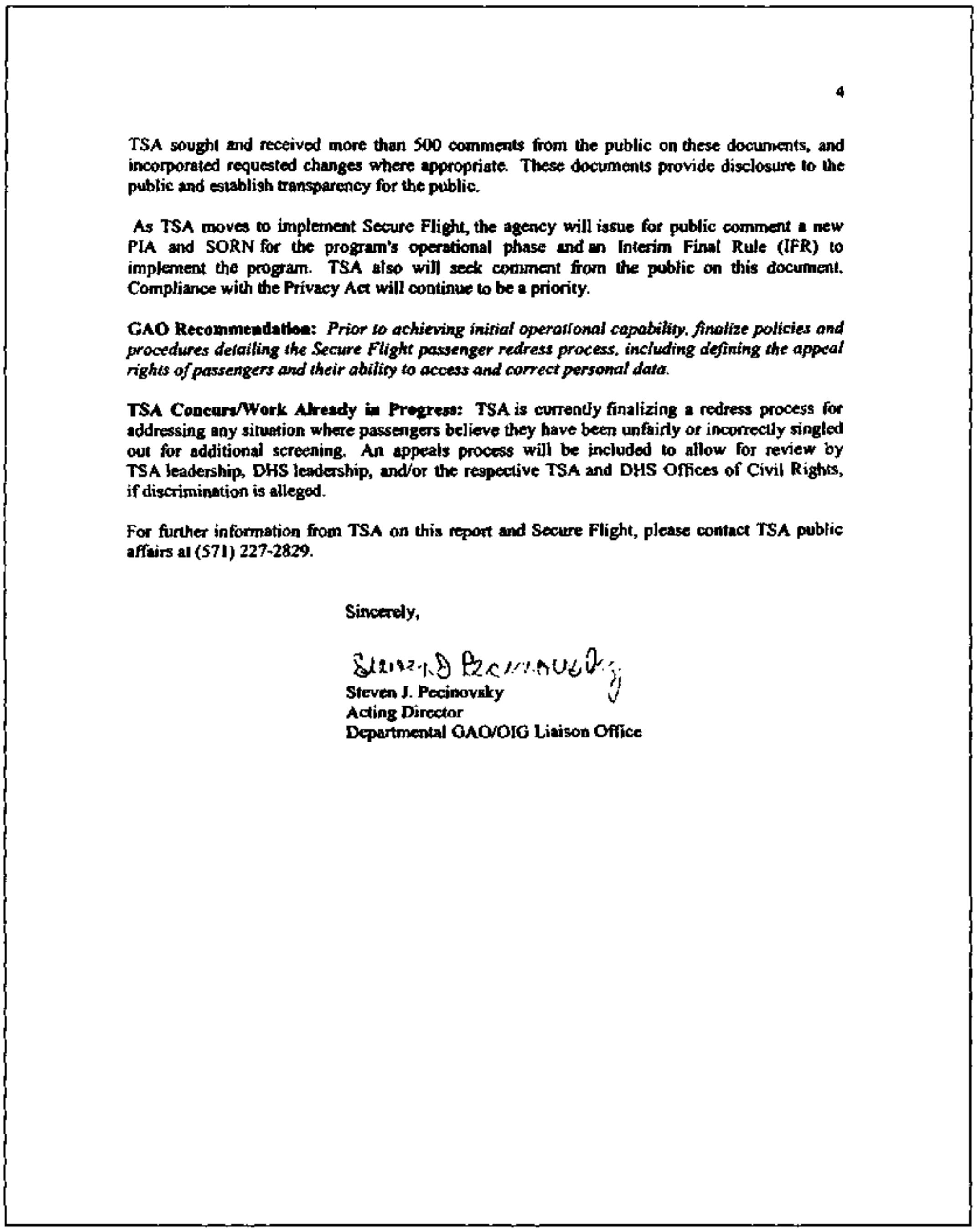
GAO Recommendation: *Develop results-oriented performance goals and measures to evaluate the effectiveness of Secure Flight in achieving intended results in an operational environment—as outlined in the Government Performance and Results Act—including measures to assess associated impacts on aviation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

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

January 17, 2007

Commissioner W. Ralph Basham
U.S. Department of Homeland Security
U.S. Customs & Border Protection
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Re: Automated Targeting System

Dear Commissioner Basham:

On November 2, 2006, the Department of Homeland Security's Privacy Office published a Federal Register Notice, hereinafter referred to as the "SORN" (71 Fed. Reg. 64543) in an effort to provide expanded notice and transparency to the public regarding Custom and Border Protection's intention to continue utilizing the Automated Targeting System - Passenger (ATS-P) to screen passengers traveling in and out of the United States. I have since learned that this system, built on its predecessor the Treasury Enforcement Communications System (TECS), has been in existence, with respect to individuals, since approximately 1999, without any prior public notice. Following this revelation, several concerns arose with respect to the program which resulted in my staff traveling to the National Targeting Center to tour its facilities, meeting with representatives from the Government Accountability Office and the DHS Privacy Officer and a subsequent meeting with CBP representatives to further explore possible privacy and civil liberties violations arising out of the use of ATS-P. I appreciate CBP's assistance throughout this process, including its cooperation with my request to extend the public comment period to allow for further evaluation.

Although some of our concerns were alleviated following the afore-mentioned meetings, there still remain questions concerning the operation of ATS-P. I believe that the answers to the following questions are vital to further understanding the nature and implications of ATS-P. My questions fall under four main areas.

I. The "risk assessment" portion of the process

1(a) Contradictory information exists regarding the use of an actual score to determine an individual's risk level. Is the individual given a score to assess risk or is there another measurement used to assess an individual's level of risk? If another measurement is used, please describe the method utilized.

1(b) Are there any sources of information, outside of government systems, that the risk assessment uses other than the passenger name records (PNRs) provided by the airlines?

1(c) Does the risk assessment process check commercial databases, which may contain records of passenger's past addresses, businesses and travel history?

1(d) If a passenger is on neither the no-fly list nor the automatic selectee list, could ATS-P produce a high enough risk assessment to bar the passenger from flying? If so, would the passenger then be placed on one of the watchlists? If the answer to the preceding is in the affirmative, what is the process governing watchlist placement? Would your answer vary, depending on whether the passenger is a U.S. citizen?

1(e) Does the system contain mechanisms that allow Passenger Name Record information to be automatically blocked from the data used to determine the risk assessment? Is this done, and which data elements are blocked? Are there any means by which this information can still be seen by CBP officials?

1(f) Examples of data that can be listed under OSI include, the language the passenger speaks, the purpose of the trip, disability status, etc. If the risk assessment increases based on based on factors, such as language and dietary restrictions, what mechanisms do you have in place to prevent racial and ethnic profiling and/or discrimination?

1(g) The SORN indicates that the system is used when an individual may pose a risk to border security, may be a terrorist or suspected terrorist, *or may otherwise be engaged in activity in violation of U.S. law.* (emphasis added) With respect to the latter, if the violation does not fall under the jurisdiction of CBP, how would the situation be handled? Does CBP have jurisdiction to enforce laws that do not fall under its purview? Please clarify how the term "engaged" is defined under these circumstances? Please provide specific examples that illustrate under what circumstances this provision would be applicable?

1(h) To what extent, if any, will CBP make Congress aware of results of using ATS-P? Will CBP report to Congress and/or the public whether using the system has led to arrests or provide data on the number of individuals who are prohibited from boarding an aircraft as a result of ATS-P information?

2. Accessibility of Information Contained within the System

2(a) Under what circumstances, if ever, is the information contained within ATS-P wholly accessible by agencies other than CBP?

2(b) If ATS-P information is accessible by sources outside of DHS, is the information made available by reference to an individual passenger, or can the information obtained through requests involve the grouping of categories of individuals? If information is made available through grouping of categories, please give examples by which the information can be grouped.

2(c) If the stated purpose of ATS-P is to target individuals who may pose a risk to border security, be a terrorist or suspected terrorist, or otherwise be engaged in illegal activities, what is the legal authority for CBP sharing ATS-P data, as a routine use, with what is broadly described as contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government?

2(d) The Federal Register Notice indicates that ATS-P data can be shared with "third parties" during the course of law enforcement investigations, without any meaningful limitations stated. What is the justification for using the ATS-P data in this fashion?

2(e) Are there any Memoranda of Understanding or other formal mechanisms in place to prevent the "third parties" referenced in the Notice from further disseminating ATS-P data? Do third parties with access to the data retain, store or aggregate the data?

3. Process for Correcting and Detecting Mistakes

3(a) The SORN states that individuals will not be able to request access to ATS-P records to determine the accuracy of the information contained within the system or request modifications if inaccurate information is contained in their individual record. In the event that an individual believes that ATS-P information, as it relates to that individual, is inaccurate, what redress, if any would the individual have? Will it be possible for the individual to have his or her information permanently corrected, to avoid repeated delays throughout the duration of the retention period, which could, according to the notice, last for forty years?

3(b) The SORN essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about them. If individuals are not able to access records and request modifications, how will the system address mistakes that may exist?

4. Retention of Information

4(a) Has the National Archives and Records Administration approved a records schedule for ATS-P records and if so, how long do they suggest records should be maintained?

4(b) What was the basis for CBP's determination that the potential active lifespan of individuals associated with terrorism or other criminal activities is forty years? Was the Department of Justice, and/or any of its components, consulted in arriving at this determination?

4(c) The SORN states that ATS-P is exempt from the Privacy Act provision that states that an agency shall only maintain information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. What is the justification for exempting ATS-P from this requirement?

Thank you, in advance, for taking the time to answer these timely questions and for your cooperation on this matter. If you have any questions, please do not hesitate to contact Jessica Herrera-Flanigan, Democratic Staff Director & General Counsel, at (202) 226-2616.

Sincerely,

Bennie G Thompson

Bennie G. Thompson
Chairman-elect
Committee on Homeland Security

Congressional Testimony

2003

Jayson Ahern, Written Testimony, Hearing before House Judiciary Committee, Subcommittee on Immigration, Border Security, and Claims (May 8, 2003)

"ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags". . . ."

John Heinrich, Written Testimony, Hearing before House Committee on International Relations, Subcommittee on International Terrorism, Nonproliferation and Human Rights (July 28, 2003)

"The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags". . . ."

Robert Bonner, Written Testimony, Hearing before House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security (October 16, 2003)

"Our National Targeting Center in Virginia is an essential tool for carrying out our priority mission.

The Center gathers the advance electronic information I talked about, and uses our Automated Targeting System for passengers and cargo to identify what is high risk – to identify potential terrorists and terrorist targets for follow up at U.S. ports of entry and CSI ports

The National Targeting Center has given us the ability to locate and eliminate terrorist threats before they become a reality, and it did not exists on 9-11."

2004

Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004)

"The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

The funding increase sought for ATS in the FY '05 budget will allow for the continued improvement of the system as well as provide it with the capacity to process the electronic data related to the ever-increasing number of people and goods entering the United States. For example, the funding will allow us to develop and implement a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. It will also be used to upgrade our passenger targeting system by improving the amount of government data that the system can access and analyze as well as provide us with the capacity to train more people on the use of the system. On the cargo side, the funding will permit ATS to increase its capacity and upgrade its capabilities by utilizing cutting edge information analysis technologies developed by CBP and the private sector."

Robert Bonner, Written Testimony, Hearing before Senate Appropriations Committee, Subcommittee on Homeland Security (March 30, 2004)

The funding sought for ATS in the FY '05 budget will allow for the continued improvement of the system as well as provide it with the capacity to process the electronic data related to the ever-increasing number of people and goods entering the United States. For example, the funding will allow us to develop and implement a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. it will also be used to upgrade our passenger targeting system by improving the amount of government data that the system can access and analyze as well as provide us with the capacity to train people on the use of the system.

Robert Bonner, Written Testimony, Hearing before House Committee on Ways and Means, Subcommittee on Trade (June 17, 2004)

The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information...

...The funding sought for ATS in the FY '05 budget will allow for the continued improvement of the system as well as provide it with the capacity to process the electronic data related to the ever-increasing number of people and goods entering the United States. For example, the funding will allow us to develop and implement a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. it will also be used to upgrade our passenger targeting system by improving the amount of government data that the system can access and analyze as well as provide us with the capacity to train people on the use of the system.

Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004)

The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

<u>2005</u>

Questions For the Record, Hearing before Senate Judiciary Committee, Subcommittee on Immigration, Border Security and Citizenship and Terroristim, Technology, and Homeland Security (March 14, 2005)

Q02411: Question: Frontline inspectors, including border officials and border patrol need to be users and collectors of terrorist travel intelligence. Are frontline personnel not only receiving the intelligence, but collecting what they are seeing in the field and relaying that information and their observations to the appropriate authorities?

Answer: CBP

Yes. Frontline personnel are receiving intelligence and are collecting what they are seeing in the field and relaying that information and their observations as appropriate. CBP has a layered reporting mechanism in place that includes reporting supported by automation, chain of command, and the National Targeting Center.

CBP frontline personnel will record their discoveries via our automated systems such as through the Automated Commercial System, Treasury Enforcement Communication System and ENFORCE. Each system has valuable information relay capabilities that once the information is in the system, all personnel with the appropriate clearances are able to immediately access and utilize the data. Additionally, specific notification capabilities exist that allow field personnel to direct the information and observations of the memorandums of information received (MOIRs) to the Intelligence Division within CBP. Also when significant activities occur within the field locations the field managers are required to report the activities to the CBP situation room located in HQ. Enhancing CBP's communication capabilities even further is the National Targeting Center. When field officers identify potential terrorists, associates of terrorists, or even suspicious shipments, the National Targeting Center is available 24 by 7 for them to call and have supporting research and coordination conducted with other government agencies. The National Targeting Center is an established field resource. The NTC began around-the-clock operations on November 10, 2001, with a priority mission of providing tactical targeting and analytical research support for Customs anti-terrorism efforts. As border inspectional assets from Customs, the Immigration and Naturalization Service, and the Department of Agriculture came together on March 1, 2003, under the umbrella of U.S. Customs and Border Protection (CBP), the NTC mission broadened commensurately with the CBP role in support of Homeland Security.

In addition to being a 24 x 7 anti-terrorism targeting center that supports Customs and Border Protection (CBP) field ports of entry, NTC coordinates with other U.S. government agencies for anti-terrorism.

· NTC targets passengers, cargo and conveyances possibly linked to terrorism
· NTC uses the Automated Targeting System (ATS) to mine regulatory databases and cross reference law enforcement databases to generate targets based upon actionable intelligence
· NTC conducts "sweeps" to proactively screen arriving passengers and cargo shipments using actionable intelligence to identify high-risk targets

Taken in context of this effort, the National Targeting Center represents the interoperability between border security and ports which is best described in its mission, scope, and general operations.

NTC Mission:
The NTC's mission is to provide tactical targeting & analytical research support for CBP anti-terrorism efforts.

Mission Scope:
The NTC is the single CBP Center for Anti-terrorism Activities, Centralizing research and support for the field. Also it is a link to the Investigative Agencies such as ICE and JTTF. Finally, it is a central location for coordinating with other government agencies at an operations-to-operations level.

Objectives:
The mission objectives of the National Targeting Center include:
1. Conducting Tactical Targeting
2. Identifying Actionable Targets
3. Generating Advanced Queries
4. Developing Sweeps and Automated Systems
5. Providing CSI Support
6. Performing Analytical Research

7. Developing Leads for Investigations
8. Coordinating with Other DHS Offices
9. Coordinating with Other Federal Agencies
10. Coordinating with Other Governments

General Staffing, Support and Liaison Operations:
· Primarily staffed by CBP Officers and Field Analysis Specialists
· Representatives from nearly all CBP disciplines are included in NTC operations
· Examples include the U.S. Border Patrol, Office of Intelligence, and other field personnel including CBP Officers, and import specialists
· The NTC staff develops tactical targets from raw information to detect and prevent terrorists and implements of terrorism from entering the United States
· NTC also supports CBP field elements, including foreign-based Container Security Initiative personnel
· The NTC provides targeting expertise to the Department of Homeland Security Operations Center
· Liaison staff from the law enforcement and intelligence communities
· During FY 2003, liaison was developed with the:
· Office of Naval Intelligence
· Transportation Security Administration
· Department of Energy
· December 8, 2003 – CBP Office of Information and Technology, Laboratories and Scientific Services (LSS) opened the Radiation Portal Monitor and Tele-forensics Center at the NTC
· December 11, 2003 – Food and Drug Administration Prior Notice Center commenced around-the-clock joint targeting operations at the NTC in support of the Bio-Terrorism Act

Working together with CBP law enforcement and regulatory counterparts internal and external to the Department of Homeland Security, the NTC and its mission continue to evolve as a cornerstone in the war on terrorism. Centralized NTC targeting endeavors, combined with intra and interagency collaboration, assure CBP of a coordinated national and field response to terrorist and national security events.

B. Terrorist Travel Specialists

It is clear from the 9/11 Commission Report and the Terrorist Travel staff report that we need some frontline personnel who are trained as terrorist travel specialists, and who have intelligence clearance, so they can be in real time contact with the intelligence community.

Q02412: Question: Do you have specialists trained in terrorist travel? If not, wouldn't you agree that there a need for specialists with clearances who can be in real time contact with the intelligence community?

Answer: CBP

Customs and Border Protection (CBP) certainly does agree with the need for specialists in terrorist travel who can talk with the intelligence community, to ports of entry that are admitting travelers 24/7, with government officials who need specialized data quickly, and provide other services that help to protect our country. But not all terrorists have been identified and the government needs to cast a wider net than looking only at the individual terrorists already ferreted out.

CBP has taken steps to meet the need described. Since many terrorists use fraudulent documents to travel --because they do not want to reveal their identities or do not qualify for travel documents in their own names -- we have organized the Fraudulent Document Analysis Unit

(FDAU) where all the fraudulent travel documents apprehended at ports of entry are sent. This unit then analyzes the kinds of fraud being perpetrated, to look for trends, common features, and keys to identifying other fraudulent documents, and to discover who may be terrorists among these malefactors. The unit is new and just beginning to make meaningful connections with the intelligence community, integrate itself with other branches of CBP, DHS, and the rest of the Federal Government. The FDAU is in operation and beginning to serve the unique function that our resources, the fraudulent documents apprehended across the United States, allow us to carry out.

Additionally, CBP has specialists trained in terrorist travel both in the Office of Field Operations and in the Office of Intelligence (OINT). The analysts in OINT have acquired an expertise in terrorist travel through a variety of training, both formal and on-the-job. They work closely with the OFO officers and provide current intelligence to them. As an example, analysts in OINT who have an expertise in terrorist travel, are in dialog on an almost daily basis with the OFO officers responsible for monitoring and amending rules used in ATS-P for automated targeting. Together decisions are made on how to translate current intelligence into rules. If it is decided that rules modifications are not applicable, OFO and intelligence analysts work together in developing special field operations to react to the intelligence that might be too broad to incorporate into rules.

With regard to real time contacts with the intelligence community, the analysts in OINT have that connectivity in a variety of ways, to include electronically and telephonically. In addition, OINT has an analyst assigned as a liaison officer.

The liaison officer, like the analysts, has gained expertise in terrorist travel through job training. The liaison officer works on-site with Office of Field Operations officers and is in daily contact with the intelligence community seeking and providing information, clarification, and recommending changes to current intelligence on terrorist travel.

Questions For the Record, Hearing before House Judiciary Committee (March 15, 2005)

10. What steps does CBP undertake that passengers and crew are adequately screened at seaport entries? Does CBP coordinate with the Terrorist Screening Center?

Answer: CBP rigorously screens watch list names from airlines and ships (both crews and passengers), destined to the United States transmitted in advance as mandated by law, through two systems, the Interagency Border Inspection System (IBIS) and Automated Targeting Systems (ATS). IBIS and ATS employ different algorithms to produce potential matches which require additional vetting either prior to or upon arrival.

Likely or positive matches are first coordinated with the Terrorist Screening Center (TSC), which serves as the government repository for watch list information, under HSPD-6, for the screening of names across all agencies of the United States Government. The TSC affirms the hit as a match, not a match or inconclusive. Both matches and inconclusive findings result in notification to the Counterterrorism Watch (CT Watch) at the National Counterterrorism Center (NCTC), which directs the Joint Terrorism Task Force (JTTF) squads around the United States. In a collaborative manner, decisions about both identification and admissibility are made between CBP and JTTF agents, though CBP alone exercises the authority to admit or refuse non-citizens at a Port of Entry (POE). Identification in advance, coordination with the TSC and CT Watch, and admissibility of all terror watch list cases at POEs are resolved through the CBP's National Targeting Center, which channels all field-level hits and maintains close communication with both TSC and CT Watch. In this way, there is a single CBP entity with awareness of all such hits at the more than 300 POEs in the United States, Canada, the Caribbean and Ireland.

Robert C. Bonner, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (May 26, 2005)

"The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

2006

DHS Press Office, Fact Sheet on "Implementing the Multilayered Port Security Strategy" (February 24, 2006)

"*Automated Targeting System (ATS).* Serves as the premier tool for performing transactional risk assessments and evaluating potential national security risks posed by cargo and passengers arriving by sea, air, truck, and rail. Using pre-arrival information and input from the intelligence community, this rules-based system identifies high-risk targets before they arrive in the United States."

Jayson Ahern and Captain Brian Salerno, Written Testimony, Hearing before House Homeland Security Committee, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity (March 16, 2006)

"The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk caro and passengers entering the United States. ATS is the system throught we process advance manifest and passenger information to detect anomalies and "red flags" and determine which passengers and cargo are "high risk" and should be scrutinizied at the port of entry, or in some cases, overseas."

Deborah Spero, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 16, 2006)

"To meet this goal, in FY2007 we will continue to improve the Automated Targeting System's ability to idenity passengers with terrorist risk factos, extending the Immigration Advisory Program, leveraging pre-departure passenger information, and strengthening consolidated anti-terrorism inspections."

Jayson P. Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006)

"The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006)

"ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

Jayson P. Ahern, Written Testimony, Hearing before Senate Finance Committee (April 26, 2006)

"The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

Jayson P. Ahern, Written Testimony, Hearing before House Homeland Security Committee, Subcommittee on Prevention of Nuclear and Biological Attack (May 25, 2006)

"The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

Robert Jacksta, Written Testimony, Hearing before Senate Committee on Foreign Relations, Subcommittee on International Operations and Terrorism (May 31, 2006)

"Addressing any major issue at the land border presents many challenges. We have over 7,000 miles of shared borders with Canada and Mexico, and each day DHS Customs and Border Protection (CBP) Officers inspect more than 1.1 million passengers and pedestrians, including many who reside in border communities who cross legally and contribute to the economic prosperity of our country and our neighbors. Maintaining this flow is critical; however, we must be confident in our determinations of who is crossing our border. In Fiscal Year 2005, over 84,000 individuals were apprehended at the ports of entry trying to cross the border with fraudulent claims of citizenship or documents. Moreover, on an average day, CBP intercepts more than 200 fraudulent documents, arrests over sixty people at ports of entry, and refuses entry to hundreds of non-citizens, a few dozen of which are criminal aliens that are attempting to enter the United States. As the 9/11 Commission report stressed, security requirements governing travel to and from Canada, Mexico and parts of the Caribbean should be treated as equivalent to security requirements for travel to and from other parts of the world."

Robert Jacksta, Written Testimony, Hearing before Senate Commerce, Science, and Transportation Committee, Subcommittee on Trade, Tourism, and Economic Development (June 22, 2006)

"At the center of our targeting efforts is CBP's National Targeting Center (NTC), where CBP personnel use the Automated Targeting System (ATS) to analyze advance information about passengers before they arrive in the United States. The NTC employs sophisticated risk assessment rules and algorithms based upon strategic intelligence about terrorist threat, and incorporates data from numerous national intelligence and law enforcement databases to screen all passengers traveling to the United States for potential terrorist connections to terrorist risk factors.

"The Immigration Advisory Program (IAP) extends our zone of security outward by screening overseas passengers before they board aircraft destined for the United States. IAP teams identify high risk and terrorist watch listed passengers using the Automated Targeting System in CBP's National Targeting Center, and advise the airline whether the passenger will be admissible to the United States upon arrival."

Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006)

"Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

Reponse to question from Sen. Kyl during hearing:

"And although is a largely compliant population of travelers, we actually had 565,417 people, individuals that were found to be inadmissible to the United States for a variety of adverse reasons. But most alarming is the fact that CBP had detected 493 of these individuals to be inadmissible under suspicion of terrorist or security grounds. These include in addition to the thousands of other arrests that we make at our ports of entry for narcotics and other violations of law also include 7,662 criminals that are queried through the national crime information database. "

Gregory Passic, Written Testimony, Hearing before Senate Finance Committee (September 12, 2006)

"Expand the Automated Targeting System (ATS) presently used for imports, exports and air passengers for use on land vehicles. Work with other federal partners in identifying suspect drug and money smuggling vehicles and subjects associated with active drug investigations. Initiate additional targeting of outbound vehicles suspected of transporting cash."

<u>Congressional Reports</u>

Department of Homeland Security Appopriations Bill, 2006, Senate Report 109-83, June 16, 2005

Targeting Systems - automated targeting system/passenger $1,500,000

Department of Homeland Security Appropriations Bill, 2005, Senate Report 108-280, June 17, 2004:

automated targeting system/passenger, $9,592,000
automated targeting system-passenger/reservations monitoring, $2,450,000

CRS Reports

RL 32840

Border and Transportation Security: Selected Programs and Policies (entire document discussing passenger screening)

RL 32399

A risk assessment system is employed to focus customs inspections on high risk shipments. The Automated Targeting System (ATS) automatically flags the shipments deemed to be the highest risks. ATS standardizes bill of lading and entry summary data received from ACS and creates integrated records called "shipments." These shipments are then evaluated and scored by ATS using weighted rules derived from the targeting methods of experienced personnel. The higher the score, the more attention the shipment requires, and the greater the chance it will be targeted for secondary inspection. ATS sorts through records stored in a database containing detailed information on every shipment that has entered the United States in the past 10 years. According to CBP, all national security related targeting using ATS is done at CBP's National Targeting Center (NTC). When a high risk shipment is flagged
by the NTC, this information (flag) is sent out to the field terminals so that when an inspector at the border pulls up information on the shipment the flag is displayed and the inspector will target the shipment for further inspection or review.

RL 33351

Foot Note 196: CBP's Passenger Analysis Unit is an automated targeting system, located at ports of
entry, that is based on strategic intelligence about threats. This system identifies individuals who may need to be more closely scrutinized.

ES # 06-5081.30

Passenger Name Records

Talking Points:

- Emphasize the criticality of PNR data for efficient border screening, particularly for passengers from VWP countries. (Only if necessary: remind the listener of the legal basis under U.S. (ATSA) and international (Chicago Convention) law).
- PNR is primarily used by U.S. Customs and Border Protection to screen all passengers flying between the United States and a foreign place to identify persons who pose a high risk for terrorism and serious crimes. The diversity of data in a PNR allows for analysis to identify possible ties to suspected terrorist or other criminal activity.
- [redacted] b7E b2 high
- PNR data is particularly valuable as a counter-terrorism tool because it provides us with information not available on the manifest that allows us to make connections between known threats and associates who we have not previously been identified as associated with terrorist activity. It allows us to look for suspected patterns of activity. It's important to note that when I say we are looking for patterns we are not profiling people based on the meal preferences, the number of beds in their hotel room, the religion etc. However, at times investigations show a pattern of activity that can help us identify guilty parties. For example that airline ticket counter agents are adding bags filled with illicit material such as drugs or weapons to an innocent traveler's reservation and coconspirators are removing these extra bags as they are unloaded from the plane.
- In our efforts to combat terrorism, drugs, human smuggling and sex tourism, for example, we have frequently been able to identify other cohorts of known criminals on the same or other flights, supporting numerous arrests. CBP is the primary user of PNR data, although DHS's border investigative arm, Immigration and Customs Enforcement has more limited but equally powerful experience with using the data.

PNR Success Stories

Aviation & Border Security

- On [redacted] a suspect [redacted] identified as traveling from [redacted] to [redacted] via [redacted] Upon pulling his PNR, b2 high b7E

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs, PLCY/OIA
Contact: [redacted]

another traveler was identified as traveling on the same reservation. DHS had no previous derogatory records on the second passenger. The [redacted] was removed from the United States and second subject was allowed to withdraw his application for admission. Similar cases have been found from [redacted] and [redacted]

- A series of PNR's generated by [redacted] in March 2005 identified linkages [redacted]

- [redacted]

b2 High
b7E

- On [redacted] CBP used PNR to identify linkages between an [redacted] on the No-Fly list and a traveler [redacted]

- On March 11, 2005 CBP arrested two individuals for smuggling drugs from London to Chicago. Upon analyzing their PNR the use of a common credit card was found. Further analysis of this credit card's reservation history found a 3rd traveler had used the same card and listed a second credit card. Analysis of this new credit card number identified 3 additional travelers. 3 of the 4 new travelers where arrested during subsequent travel with drugs.

- On [redacted] CBP analysis of PNR for a flight from [redacted] to Chicago identified 3 ← b2 High b7E passengers that may have been seeking to use fraudulent travel documents. CBP alerted the air carrier who performed a thorough review of all three travelers documents prior to boarding. One was denied boarding by the airline. The two remaining travelers were referred to CBP secondary upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were smugging the first subject. Additionally, one subject was identified as a member of the Yazuka crime syndicate.

- In January 2003, CBP Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. In this instance a corrupt ticket counter agent would identify a low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.

- CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in Costa Rica. [redacted] b2 High b7E

Transnational Crimes

- ICE used Dominican PNR to identify and dismantle a human smuggling ring between the Dominican Republic and the United States. In this case 7 women were traveling to the United

States with children other than their own under their own children's passports. Through an analysis of the first suspects PNR a pattern in which the children constantly did not make the return flight was identified. By looking for this pattern, DHS identified the remaining 6 smugglers. Once the suspects were identified, lookouts were placed in APIS for pending arrivals. Ultimately this case resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique.

- Upon identifying a suspected sexual predators intent to travel to Bangkok, ICE was able to identify two travel agencies specializing in sex tourism and a number of other predators traveling to Asia for the same purpose. Through this ongoing case ICE has identified reservation patterns employed by sex tourism companies, including diversification of flight reservations culminating in a central location. It also facilitated ICE's ability to marshal surveillance resources by monitor the individual's movements.
- ICE has also used PNR to identify coconspirators of individuals on a watchlist. Through APIS data CBP identified a suspected Venezuelan heroin smuggler due to arrive in the United States. By analyzing PNR, a second individual was found to be traveling on the same reservation and was also arrested with drugs.
- ICE was also able to use PNR to support the early identification of a money launder for the Hells Angels Motorcycle Gang. Investigatory intelligence indicated that this individual was due to make a brief stop in New York City while traveling between the Caribbean and Canada. PNR was able to allow ICE to identify, in advance, the airport he would be arriving into, arange for him to be followed to a criminal meeting and be arrested. If ICE had been limited to APIS data in this case it is likely that they would not have had enough lead time to make the arrest.
- ICE has also used PNR to reinvigorate a variety of cases in which critical evidence was tied to telephone numbers with fictitious subscriber data. Since criminals used these phone numbers in making travel reservations, ICE was able to identify valid leads as well as to clear individuals who's names were used unbeknownst to them in phone service provider records.

<u>Watch Out For/If Asked:</u>

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs, PLCY/OIA
Contact: [illegible]

Background:

Passenger Name Record is a generic name for that information that may be collected from each passenger by travel agents and airlines and stored in their record systems for the purpose of managing a flight. While the record held by each carrier can vary dramatically, it typically includes information such as name, contact information, payment method, information about a traveler's baggage. PNR differs significantly from Advance Passenger Information System (APIS) data, which is developed from the carriers manifest and is largely derived from the information on the traveler's passport. APIS data is confirmed biographic data while PNR includes preliminary biographic information and other transactional data elements by which a person or activity may be identified.

The former U.S. Customs Service (now, U.S. Customs and Border Protection) began using PNR from air carriers on a voluntary basis in 1996, initially in an effort to facilitate the clearing of low risk travelers – a function it still serves today. However, after the terrorist attack on September 11, 2001, Congress required the U.S. Customs Service to mandate access to PNR data to support its border security screening, particularly to identify persons who may constitute a high risk for terrorism. (**Background note:** 1996 is the first year Customs began collecting PNR data in an automated system. In 1992 we Customs worked with the airlines to screen PNR data via their computer systems located in the airline's offices at each airport.)

Consistent with the Aviation and Transportation Security Act of 2001, each air carrier operating passenger flights in foreign air transportation to or from the United States must provide the Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) with electronic access to passenger name record (PNR) data to the extent it is collected and contained in the air carrier's automated reservation departure control systems ("reservation systems"). In 2002, the EU raised concerns that the statutory requirement conflicted with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("European Data Protection Directive"). Most significantly, the European Data Protection Directive places burdens on private sector data controllers that limits their ability to share personal data across international borders with non-EU countries absent a demonstration that the receiving entity in a third country has adequate data protection standards.

In 2004, the United States government reached an arrangement with the European Commission (EC) which permitted airlines to legally provide access to passenger name record (PNR) data emanating from within the European Union (EU) to CBP. This access is subject to carefully negotiated limitations as set forth in a set of Undertakings issued by CBP offering detailed assurances on how the DHS component would collect, process, handle, protect, share and ensure oversight of PNR data received in connection with flights between the U.S. and EU. Compliance

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs, PLCY/OIA

Contact: b 2 3

with the Undertakings required significant system, policy and operational modifications by CBP and was accomplished on May 13, 2005.

The PNR Case. Shortly after the 2004 signing of the European Union agreement on CBP access to Passenger Name Record data, the European Parliament (EP), disturbed over what it viewed as an attack on personal privacy and its own authority, filed two suits in the European Court of Justice (ECJ) against the actions of the European Commission (EC) and the European Council for entering into the information sharing arrangement. The first suit challenged the authority of the EC and the European Council to enter into the International Agreement without the assent of the Parliament; the second challenged the merits of the arrangement itself - whether the Undertakings were adequate to meet the information privacy protections afforded under EU law to all individuals.

On May 30, 2006 the European Court of Justice (ECJ) annulled the decision of adequacy made by the European Commission, as well as the European Council's decision to enter into an international agreement with DHS on the use of Passenger Name Records. In issuing this finding, the Court did not rule against the availability of PNR data, it did not determine that privacy was violated, nor did it take a view on the content of the agreement. Rather, consistent with the Advocate General's November 2005 opinion, the court found that the decisions of the Commission and Council where premised upon an inapplicable legal basis under European law instead of concluding the agreement under the data protection provisions of Article 95, the court deemed that the processing of PNR data is a law enforcement and public security issue, and as a result, is a shared competency between the European Union and Member States under the so called "third pillar."

The Court's ruling gave the European Commission until September 30, 2006 to establish a new community-wide arrangement to govern PNR access for flights to the United States. However, since the ECJ's decision removes the threat of fines and criminal penalties based on EU law, the immediate consequences for not striking a new arrangement are significantly diminished.

The Interim Agreement:

On October 19, 2006, the United States signed an interim agreement (already signed by the European Union) on the processing and transfer of passenger name record (PNR) data. This agreement was accompanied by a unilateral letter of interpretation of U.S. obligations with regard to such data that was negotiated by the parties and acknowledged by the EU. This new arrangement – which will expire on July 31, 2007 enables DHS to share information in ways that were not possible under the previous interpretation of the May 11, 2004 Undertakings, which formed the basis of the earlier U.S.-EU arrangement. It also codifies certain assumptions associated with the Undertakings including: carriers obligations in migrating to a system in which they transmit data to CBP, that a joint review is not necessary between the signing and the expiration of the agreement, access to additional data in the frequent flier field, and the use of sensitive information to protect the vital interests of the data subject. Nonetheless the agreement continues many of the deficiencies of the original 2004 agreement, including an overly short retention period, a facilitated but still disjointed regime for sharing PNR within the USG and does not allow for passenger participation through notice and consent. In addition, the detailed nature of the agreement, which is premised on EU oversight of DHS activities, limits the ability of the United States Government to adapt to changing requirements in combating terrorism and crime. DHS is in the process of discussing potential replacements with the EU with a goal of concluding such talks before July 31, 2007.

Prescreening Systems of Other Governments:

Presently most nations do not collect PNR in order to prescreen travelers. Canada, however, does collect PNR and has an agreement with the EU similar to the 2004 U.S.-EU Agreement. In fact, the EU typically holds their agreement with Canada up as more of a model than their agreement with the United States. In addition, Canada shares PNR with the United States pursuant to the Shared Border Accord. Rumors persist that a number of European governments are pursuing PNR systems including the U.K., France, Spain, Italy and the EU but few details have been made available.

The use of APIS and Advance Passenger Processing (APP) data is more common. All ICC member countries collect APIS or APP data in order to prescreen travelers. The United States has cooperative arrangements with Canada and Mexico to share this type of information.

Drafted by: Michael Scardaville, Deputy Director, European and Multilateral Affairs, PLCY/OIA
Contact: [illegible]