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

February 9, 2006

AVIATION SECURITY

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

GAO Accountability·Integrity·Reliability

Highlights

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

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

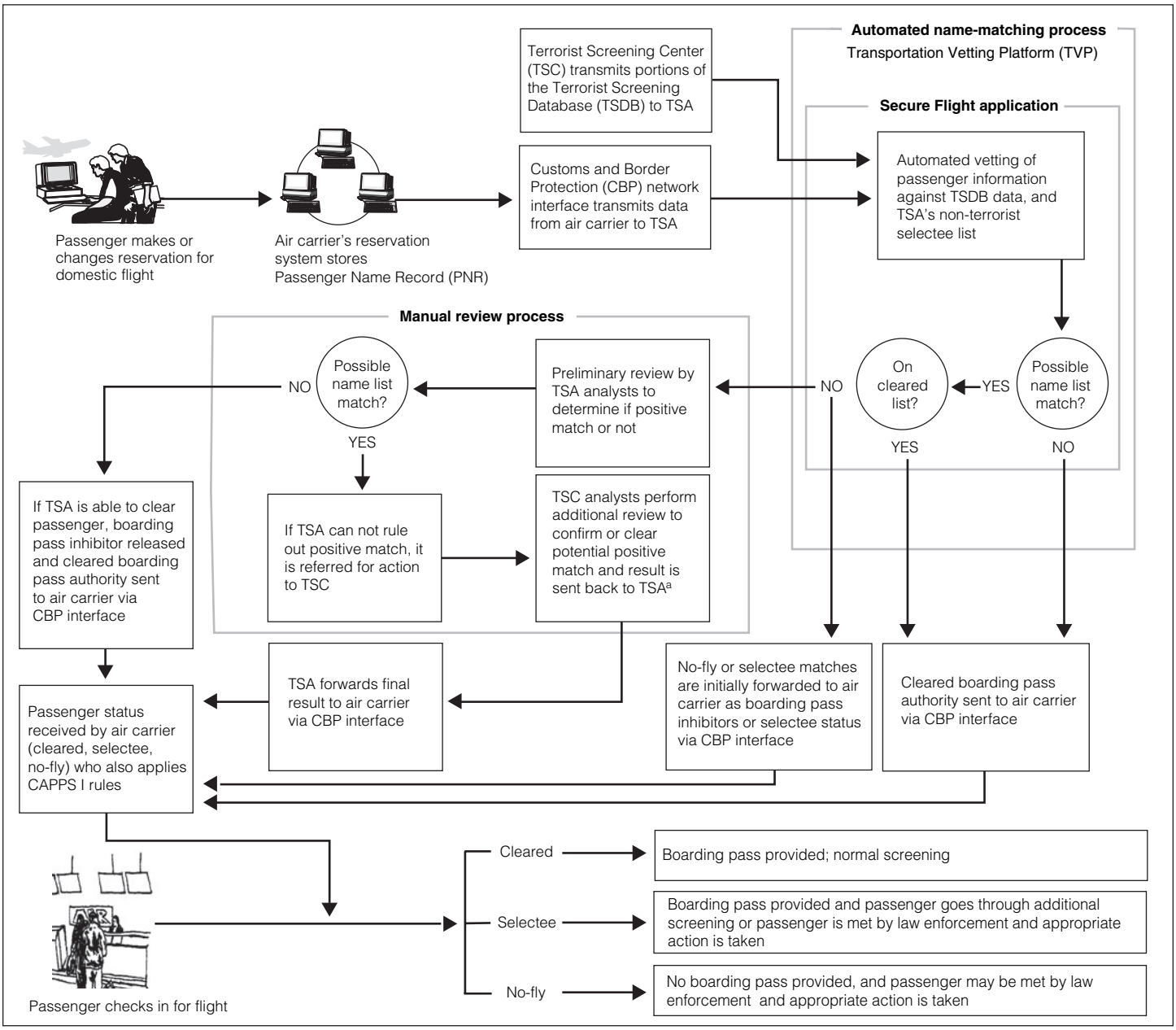
[9]This description of the Secure Flight system, as well as the graphic illustrating the system in figure1, is based on TSA's draft June 9, 2005, concept of operations, a document that gives a high-level overview of the Secure Flight system.

[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



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.

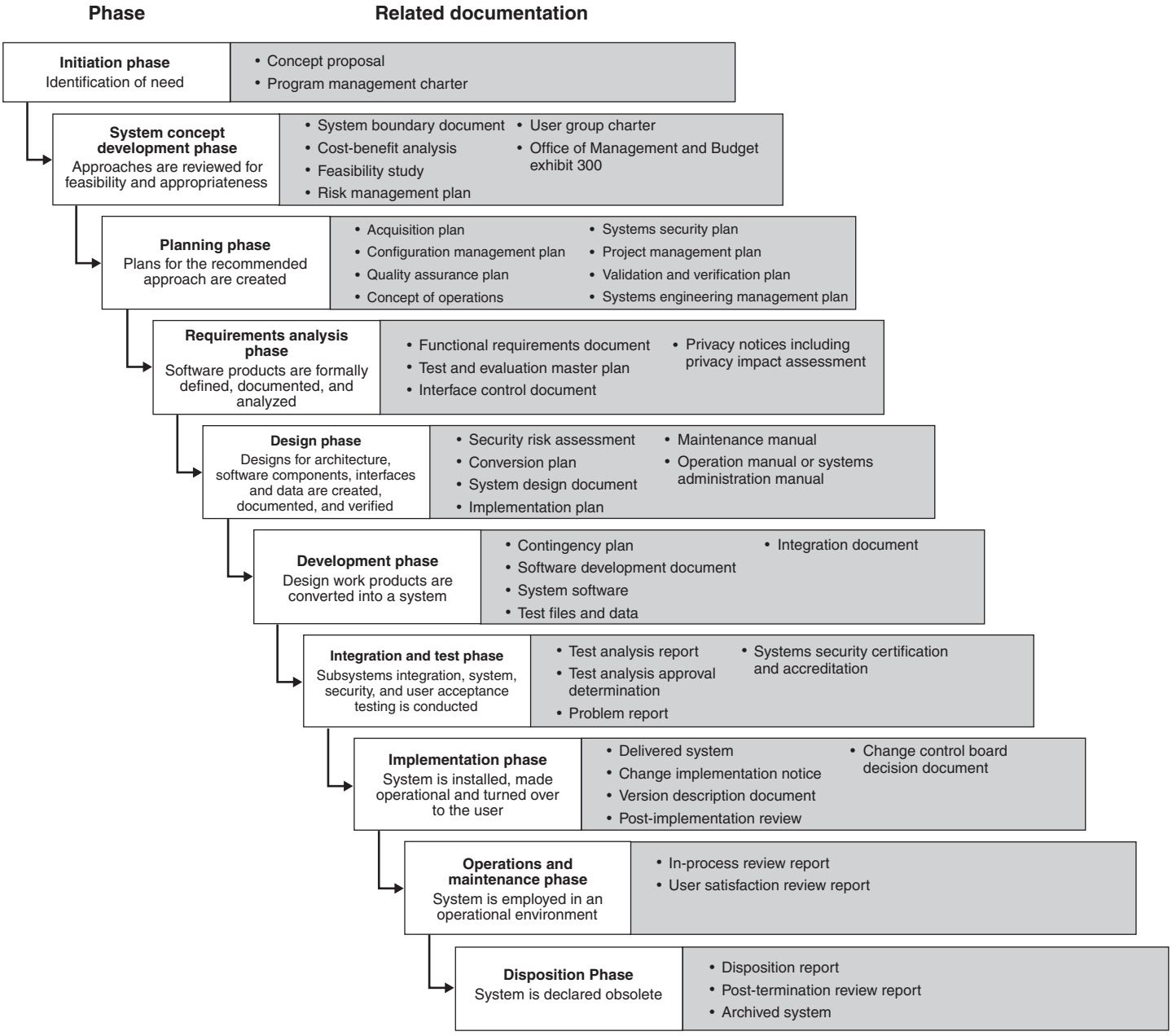
TSA Has Not Followed a Disciplined Life Cycle Process or Fully Defined System Requirements but Plans to Address These Issues

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



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.

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