United States Government Accountability Office

GAO

Report to Congressional Committees

May 2009

AVIATION SECURITY

TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks

GAO-09-292

May 2009

AVIATION SECURITY

TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-09-292, a report to congressional committees

Why GAO Did This Study

To enhance aviation security, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) developed a program—known as Secure Flight—to assume from air carriers the function of matching passenger information against terrorist watch-list records. In accordance with a mandate in the Department of Homeland Security Appropriations Act, 2008, GAO's objective was to assess the extent to which TSA met the requirements of 10 statutory conditions related to the development of the Secure Flight program. GAO is required to review the program until all 10 conditions are met. In September 2008, DHS certified that it had satisfied all 10 conditions. To address this objective, GAO (1) identified key activities related to each of the 10 conditions; (2) identified federal guidance and best practices that are relevant to successfully meeting each condition; (3) analyzed whether TSA had demonstrated, through program documentation and oral explanation, that the guidance was followed and best practices were met; and (4) assessed the risks associated with not fully following applicable guidance and meeting best practices.

What GAO Recommends

GAO recommends that DHS take action to periodically assess the performance of the Secure Flight system's name-matching capabilities and results. DHS concurred with GAO's recommendation.

View GAO-09-292 or key components.

For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov; or Randolph C. Hite at (202) 512-3439 or hiter@gao.gov; or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

As of April 2009, TSA had generally achieved 9 of the 10 statutory conditions related to the development of the Secure Flight program and had conditionally achieved 1 condition (TSA had defined plans, but had not completed all activities for this condition). Also, TSA's actions completed and those planned have reduced the risks associated with implementing the program. Although DHS asserted that TSA had satisfied all 10 conditions in September 2008, GAO completed its initial assessment in January 2009 and found that TSA had not demonstrated Secure Flight's operational readiness and that the agency had generally not achieved 5 of the 10 statutory conditions. Consistent with the statutory mandate, GAO continued to review the program and, in March 2009, provided a draft of this report to DHS for comment. In the draft report, GAO noted that TSA had made significant progress and had generally achieved 6 statutory conditions, conditionally achieved 3 conditions, and had generally not achieved 1 condition. After receiving the draft report, TSA took additional actions and provided GAO with documentation to demonstrate progress related to 4 conditions. Thus, GAO revised its assessment in this report, as is reflected in the table below.

GAO Assessment of Whether DHS Has Achieved the 10 Statutory Conditions, as of April 2009

Statutory condition topic	Generally achieved	Conditionally achieved[a]	Generally not achieved
System of Due Process (Redress)	X		
Extent of False-Positive Errors (Misidentifications)	X		
Performance of Stress Testing and Efficacy and Accuracy of Search Tools	X		
Establishment of an Internal Oversight Board	X		
Operational Safeguards to Reduce Abuse Opportunities	X		
Substantial Security Measures to Prevent Unauthorized Access by Hackers	X		
Effective Oversight of System Use and Operation	X		
No Specific Privacy Concerns with the System's Technological Architecture	X		
Accommodation of States with Unique Transportation Needs	X		
Appropriateness of Life-Cycle Cost Estimates and Program Plans		X	

Source: GAO analysis.

[a]For conditionally achieved, TSA has completed some key activities and has defined plans for completing remaining activities that, if effectively implemented as planned, should result in a reduced risk of the program experiencing cost, schedule, or performance shortfalls.

Related to the condition that addresses the efficacy and accuracy of search tools, TSA had not yet developed plans to periodically assess the performance of the Secure Flight system's name-matching capabilities, which would help ensure that the system is working as intended. GAO will continue to review the Secure Flight program until all 10 conditions are generally achieved.

Contents

Tables

Figure

Abbreviations

AO	Aircraft Operator
APB	Acquisition Program Baseline
BPPR	Boarding Pass Printing Result
CAPPS	Computer-Assisted Passenger Prescreening System
CBP	U.S. Customs and Border Protection
CSA	Customer Service Agent
DHS	Department of Homeland Security
EAB	Enterprise Architecture Board
eSecure Flight	Electronic Secure Flight
ICE	independent cost estimate
IGCE	independent government cost estimate
IMS	Integrated Master Schedule
IRB	Investment Review Board
KDP	Key Decision Point
LCCE	life-cycle cost estimate
MDP	Milestone Decision Point
NARA	National Archives and Records Administration
OI	Office of Intelligence
OMB	Office of Management and Budget
OTSR	Office of Transportation Security Redress
PIA	Privacy Impact Assessment
PII	personally identifiable information
POA&M	plans of actions and milestones
PRR	Preliminary Review Required
RFA	Referred for Action
SFA	Secure Flight Analyst
SFPD	Secure Flight Passenger Data
SORN	System of Records Notice
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOU	Terrorist Screening Operations Unit
WBS	work breakdown structure

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 13, 2009

Congressional Committees

The matching of airline passenger information against terrorist watch-list records (watch-list matching) is a frontline defense against acts of terrorism that target the nation's civil aviation system. In general, passengers identified by air carriers as a match to the No-Fly list are prohibited from boarding a commercial flight, while those matched to the Selectee list are required to undergo additional screening.[1] Historically, airline passenger prescreening has been performed by commercial air carriers.

As required by the Intelligence Reform and Terrorism Prevention Act of 2004, the Transportation Security Administration (TSA) developed an advanced passenger prescreening program known as Secure Flight that will allow TSA to assume from air carriers the function of watch-list matching.[2] Since fiscal year 2004, GAO has been mandated to assess the development and implementation of the Secure Flight program.[3] Most recently, in February 2008, we reported that TSA had instilled more discipline and rigor into Secure Flight's development, but that the program continued to face challenges related to completing performance testing, fully defining and testing security requirements, and establishing reliable cost and schedule estimates.[4] We made recommendations to address these challenges and TSA generally agreed with them.

[1]The No-Fly and Selectee lists contain the names of individuals with known or suspected links to terrorism. These lists are subsets of the consolidated terrorist watch list that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

[2]See Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714-18 (2004) (codified at 49 U.S.C. § 44903(j)(2)(C)).

[3]GAO has performed this work in accordance with statutory mandates, beginning in fiscal year 2004 with the Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003) (establishing the initial mandate that GAO assess the Computer-Assisted Passenger Prescreening System (CAPPS) II, the precursor to Secure Flight, and setting forth the original eight statutory conditions related to the development and implementation of the prescreening system), and pursuant to the requests of various congressional committees.

[4]GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-456T (Washington, D.C. Feb. 28, 2008).

Section 522(a) of the Department of Homeland Security (DHS) Appropriations Act, 2005, set forth 10 conditions related to the development and implementation of the Secure Flight program that the Secretary of Homeland Security must certify have been successfully met before the program may be implemented or deployed on other than a test basis (see table 1).[5] On September 24, 2008, DHS certified that it had satisfied all 10 conditions.

Table 1: Simplified Description of 10 Statutory Conditions Related to Secure Flight

Condition 1: System of Due Process (Redress)[a]
Condition 2: Extent of False-Positive Errors (Misidentifications)
Condition 3: Performance of Stress Testing and Efficacy and Accuracy of Search Tools
Condition 4: Establishment of an Internal Oversight Board
Condition 5: Operational Safeguards to Reduce Abuse Opportunities
Condition 6: Substantial Security Measures to Prevent Unauthorized Access by Hackers
Condition 7: Effective Oversight of System Use and Operation
Condition 8: No Specific Privacy Concerns with the System's Technological Architecture
Condition 9: Accommodation of States with Unique Transportation Needs[b]
Condition 10: Appropriateness of Life-Cycle Cost Estimates and Program Plans

Source: GAO summary of the10 statutory conditions in Section 522 of Public Law 108-334 .

[a]In general, the term "redress" refers to an agency's complaint resolution process whereby individuals may seek resolution of their concerns about an agency action.

[b]Condition 9 is related to the Computer-Assisted Passenger Prescreening System (CAPPS), a TSA-mandated automated program operated by air carriers that considers characteristics of a passenger's travel arrangements to select passengers for secondary screening. CAPPS is distinct from the Secure Flight program. TSA did not incorporate CAPPS into the Secure Flight program and, therefore, Secure Flight will have no effect on CAPPS selection rates.

In accordance with section 513 of the Department of Homeland Security Appropriations Act, 2008, our objective was to assess the extent to which TSA met 10 statutory conditions and the associated risks of any shortfalls in meeting the requirements.[6] Our overall methodology included (1) identifying key activities related to each condition; (2) identifying federal guidance and related best practices, if applicable, that are relevant to successfully meeting each condition (e.g., GAO's Standards for Internal

[5]See Pub. L. No. 108-334, § 522, 118 Stat. 1298, 1319-20 (2004).

[6]See Pub. L. No. 110-161, Div. E, § 513, 121 Stat. 1844, 2072 (2007); see also Pub. L. No. 110-329, Div. D, § 512, 122 Stat. 3574, 3682-83 (2008).

Control in the Federal Government);[7] (3) analyzing whether TSA has demonstrated through verifiable analysis and documentation, as well as oral explanation, that the guidance has been followed and best practices have been met; and (4) assessing the risks associated with not fully following applicable guidance and meeting best practices. Based on our assessment, we categorized each condition as generally achieved, conditionally achieved, or generally not achieved.

- Generally achieved—TSA has demonstrated that it completed all key activities related to the condition in accordance with applicable federal guidelines and related best practices, which should reduce the risk of the program experiencing cost, schedule, or performance shortfalls.

- Conditionally achieved—TSA has demonstrated that it completed some key activities related to the condition in accordance with applicable federal guidelines and related best practices and has defined plans for completing remaining key activities that, if effectively implemented as planned, should result in a reduced risk that the program will experience cost, schedule, or performance shortfalls.

- Generally not achieved—TSA has not demonstrated that it completed all key activities related to the condition in accordance with applicable federal guidelines and related best practices and does not have defined plans for completing the remaining activities, and the uncompleted activities result in an increased risk of the program experiencing cost, schedule, or performance shortfalls.

On January 7, 2009, we briefed staff of the Senate and House Appropriations Committees' Subcommittees on Homeland Security on the results of our initial work, and reported that TSA had not demonstrated Secure Flight's operational readiness and that the agency had generally not achieved 5 of the 10 statutory conditions. Our briefing also included

[7]See GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982, provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to the 1982 act, the Office of Management and Budget (OMB) issued circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in OMB Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*. Appendix I contains more details on federal guidance and related best practices.

several recommendations for DHS to mitigate risks of Secure Flight cost, schedule, or performance shortfalls and strengthen management of the program.[8] In addition, under this mandate, GAO is required to continue to review the Secure Flight program until it determines that all 10 conditions have been successfully met. In accordance with this requirement, we conducted additional work from January through April 2009, which included assessing information DHS provided after we submitted a copy of our draft report to the department for formal agency comment. Based on this additional work, we revised the status of several conditions and now consider three of the recommendations we made in our draft report to be met. This report contains information on our initial January 2009 assessment and recommendations, and related updates through April 2009.

We conducted this performance audit from May 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I presents more details about our scope and methodology.

Background

Overview of Secure Flight

The prescreening of airline passengers who may pose a security risk before they board an aircraft is one of many layers of security intended to strengthen commercial aviation. In July 2004, the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, reported that the current system of matching passenger information to the No-Fly and Selectee lists needed improvements. The commission recommended, among other things, that watch-list matching be performed by the federal government rather than by air carriers. Consistent with this recommendation and as required by law, TSA has

[8]On December 19, 2008, we provided the initial results of our work to staff of the Senate and House Appropriations Committees' Subcommittees on Homeland Security, which was based on work conducted as of December 8, 2008. Section 513(b) of the Department of Homeland Security Appropriations Act, 2008, mandated that GAO report to these committees within 90 days after the DHS Secretary's certification.

undertaken to develop a program—Secure Flight—to assume from air carriers the function of watch-list matching. Secure Flight is intended to

- eliminate inconsistencies in current passenger watch-list matching procedures conducted by air carriers and use a larger set of watch-list records when warranted,
- reduce the number of individuals who are misidentified as being on the No-Fly or Selectee list,
- reduce the risk of unauthorized disclosure of sensitive watch-list information, and
- integrate information from DHS's redress process into watch-list matching so that individuals are less likely to be improperly or unfairly delayed or prohibited from boarding an aircraft.[9]

Statutory requirements govern the protection of personal information by federal agencies, including the use of air passengers' information by Secure Flight. For example, the Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[10] The Privacy Act requires agencies to publish a notice—known as a System of Records Notice (SORN)—in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" use of the data, and procedures that individuals can use to review and correct personal information. Also, the E-Government Act of 2002 requires agencies to conduct Privacy Impact Assessments (PIA) that analyze how personal information is collected, stored, shared, and managed in a federal system.[11] Agencies are required to make their PIAs publicly available if practicable.

Secure Flight Development and Watch-List Matching Process

According to TSA, the agency developed and is implementing Secure Flight's domestic watch-list matching function in 3 releases:

- Release 1—Systems development and testing.

[9]In general, the term "redress" refers to an agency's complaint resolution process whereby individuals may seek resolution of their concerns about an agency action.

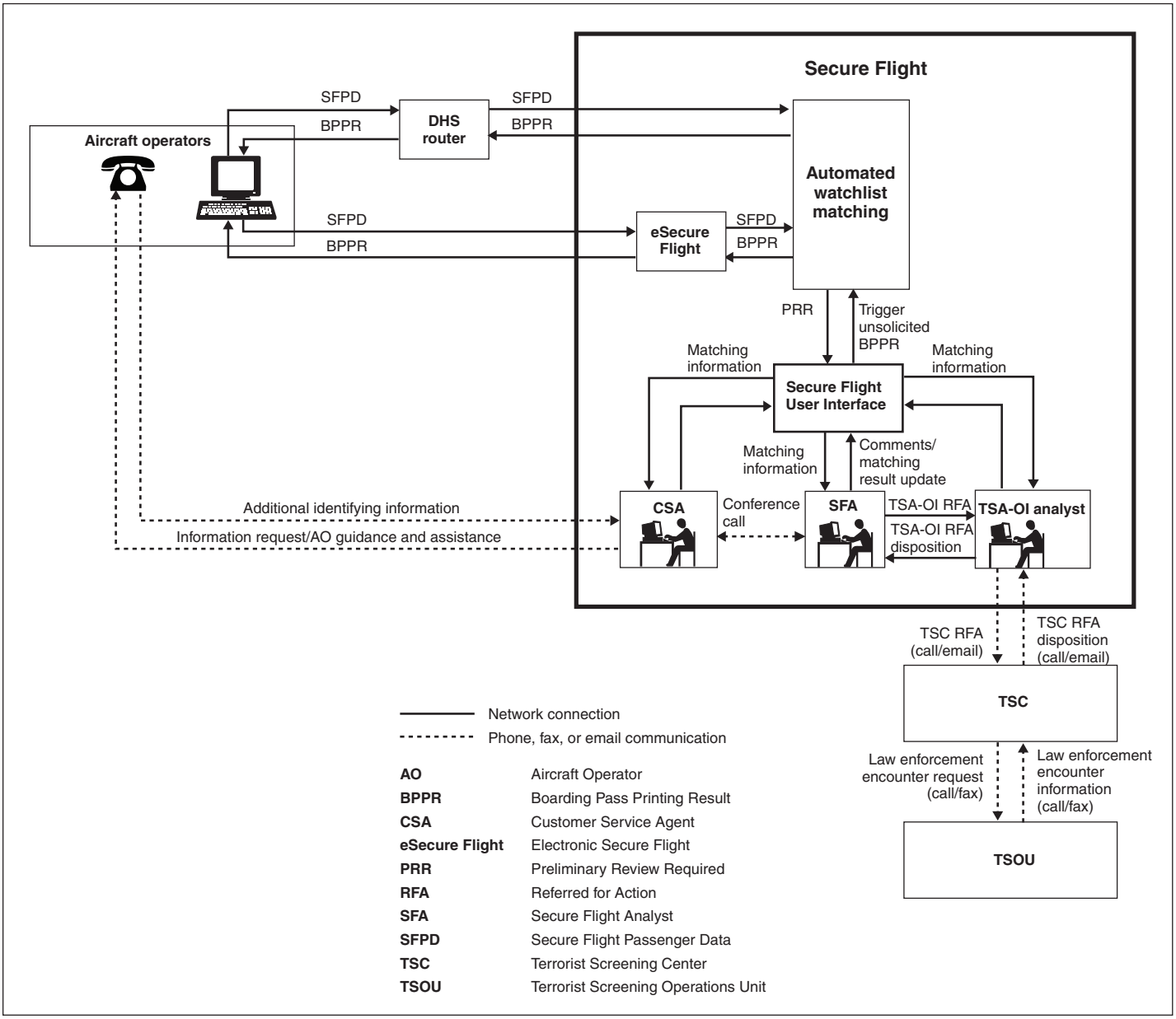
[10]See 5 U.S.C. § 552a.

[11]See Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-23 (2002).

- Release 2—First stages of parallel operations with airline operators during which both Secure Flight and air carriers perform watch-list matching.
- Release 3—Continued parallel operations with airline operators and preparation for airline cutovers, in which Secure Flight will perform passenger watch-list matching for domestic flights.

Under the Secure Flight watch-list matching process (see fig. 1), air carriers submit passenger information, referred to as Secure Flight Passenger Data, electronically through a DHS router or eSecure Flight, a Web-based access system for air carriers that do not use automated reservation systems to send and receive the data. Secure Flight Passenger Data are matched automatically against watch-list records, with results provided to air carriers through a Boarding Pass Printing Result. Passengers are subject to three possible outcomes from the watch-list matching process: cleared to fly, selected for additional screening, or prohibited from flying. Individuals initially selected for additional screening and those prohibited from flying undergo additional review, which results in the final Boarding Pass Printing Result and may lead to law enforcement involvement.

Figure 1: Secure Flight Watch-List Matching Process



Source: GAO analysis; Art Explosion.

TSA is to use discretion to determine what constitutes a possible match between passenger information and a watch-list record, based on

matching settings made in the system. The matching settings include (1) the relative importance of each piece of passenger information (e.g., name versus date of birth); (2) the numeric threshold over which a passenger will be flagged as a potential match (e.g., a scoring threshold of 95 would result in fewer matches than a scoring threshold of 85); and (3) the criteria used to determine whether an element of passenger information is a potential match to the watch list (e.g., the types of name variations or the date-of-birth range that the system considers a match). The Secure Flight matching system will use this information to assign each passenger record a numeric score that indicates its strength as a potential match to a watch-list record.

Raising the scoring threshold would result in more names cleared and fewer names identified as possible matches, which would raise the risk of the subject of a watch-list record being allowed to board an airplane (false-negative matches). Conversely, lowering the scoring threshold would raise the risk of passengers being mistakenly matched to the watch list (false-positive matches). In October 2008, TSA issued the Secure Flight Final Rule, which specifies requirements for air carriers to follow as TSA implements and operates Secure Flight, including the collection of full name and date-of-birth information from airline passengers to facilitate watch-list matching.[12]

In late-January 2009, TSA began to assume the watch-list matching function for a limited number of domestic flights for one airline, and has since phased in additional flights and airlines. TSA plans to complete assumption of the watch-list matching function for all domestic flights in March 2010 and to then assume from U.S. Customs and Border Protection this watch-list-matching function for international flights departing to and from the United States. According to TSA, since fiscal year 2004, it has received approximately $300 million in appropriated funds for the development and implementation of the Secure Flight program.

Related System Also Prescreens Airline Passengers

In addition to matching passenger information against terrorist watch-list records, TSA requires air carriers to prescreen passengers using the Computer-Assisted Passenger Prescreening System (CAPPS). Through CAPPS, air carriers compare data related to a passenger's reservation and travel itinerary to a set of weighted characteristics and behaviors (CAPPS

[12]See 73 Fed. Reg. 64,018 (Oct. 28, 2008) (codified at 49 C.F.R. pt. 1560).

rules) that TSA has determined correlate closely with the characteristics and behaviors of terrorists. Passengers identified by CAPPS as exhibiting these characteristics—termed selectees—must undergo additional security screening. This system is separate from the Secure Flight watch-list matching process and thus Secure Flight has no effect on CAPPS selection rates.

TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks

In a January 2009 briefing to congressional staff, we reported that TSA had not demonstrated Secure Flight's operational readiness and that the agency had generally not achieved 5 of the 10 statutory conditions (Conditions 3, 5, 6, 8, 10), although DHS asserted that it had satisfied all 10 conditions. Since then, TSA has made progress in developing the Secure Flight program and meeting the requirements of the 10 conditions, and the activities completed to date and those planned reduce the risks associated with implementing the program. Table 2 shows the status of the 10 conditions as of April 2009.

Table 2: GAO Assessment of Whether DHS Has Generally Achieved 10 Statutory Conditions, as of April 2009

Statutory condition topic	Generally Achieved[a]	Conditionally Achieved[b]	Generally Not Achieved[c]
Condition 1: System of Due Process (Redress)	X		
Condition 2: Extent of False-Positive Errors	X		
Condition 3: Performance of Stress Testing and Efficacy and Accuracy of Search Tools	X		
Condition 4: Establishment of an Internal Oversight Board	X		
Condition 5: Operational Safeguards to Reduce Abuse Opportunities	X		
Condition 6: Substantial Security Measures to Prevent Unauthorized Access by Hackers	X		
Condition 7: Effective Oversight of System Use and Operation	X		
Condition 8: No Specific Privacy Concerns with the System's Technological Architecture	X		
Condition 9: Accommodation of States with Unique Transportation Needs	X		
Condition 10: Appropriateness of Life-Cycle Cost Estimates and Program Plans		X	

Source: GAO analysis.

[a]For generally achieved, TSA has completed all key activities, which should reduce the risk of the program experiencing cost, schedule, or performance shortfalls.

[b]For conditionally achieved, TSA has completed some key activities and has defined plans for completing remaining activities that, if effectively implemented as planned, should result in a reduced risk of the program experiencing cost, schedule, or performance shortfalls.

[c]For generally not achieved, TSA has not completed all key activities, and the uncompleted activities result in an increased risk of the program experiencing cost, schedule, or performance shortfalls.

TSA Has Generally Achieved 9 of the 10 Statutory Conditions, but Additional Actions Would Help Mitigate Future Risks

Condition 1: Redress

Condition 1 requires that a system of due process exist whereby aviation passengers determined to pose a threat who are either delayed or prohibited from boarding their scheduled flights by TSA may appeal such decisions and correct erroneous information contained in the Secure Flight program.

TSA has generally achieved this condition. For the Secure Flight program, TSA plans to use the existing redress process that is managed by the DHS Traveler Redress Inquiry Program (TRIP). TRIP, which was established in February 2007, serves as the central processing point within DHS for travel-related redress inquiries. TRIP refers redress inquiries submitted by airline passengers to TSA's Office of Transportation Security Redress (OTSR) for review. This process provides passengers who believe their travels have been adversely affected by a TSA screening process with an opportunity to be cleared if they are determined to be an incorrect match to watch-list records, or to appeal if they believe that they have been wrongly identified as the subject of a watch-list record. Specifically, air travelers who apply for redress and who TSA determines pose no threat to aviation security are added to a list that should automatically "clear" them and allow them to board an aircraft (the "cleared list"), thereby reducing any inconvenience experienced as a result of the watch-list matching

process.[13] After a review of the passenger's redress application, if OTSR determines that an individual was, in fact, misidentified as being on the No-Fly or Selectee list, it will add the individual to the cleared list. If OTSR determines that an individual is actually on the No-Fly or Selectee list, it will refer the matter to the Terrorist Screening Center, which determines whether the individual is appropriately listed and should remain on the list or is wrongly assigned and should be removed from the list.

Although Secure Flight will use the same redress process that is used by the current air carrier-run watch-list matching process, some aspects of the redress process for air travelers are to change as the program is implemented. For example, individuals who apply for redress are issued a redress number by TRIP that they will be able to submit during future domestic air travel reservations that will assist in the preclearing process before they arrive at the airport. TSA expects this will reduce the likelihood of travel delays at check-in for those passengers who have been determined to pose no threat to aviation security. According to TSA officials, individuals who have applied for redress in the past and were placed on the cleared list will need to be informed of their new ability to use their redress number to preclear themselves under Secure Flight. These officials stated that they intend to send mailings to past redress applicants with information on this change.

TSA has also coordinated with key stakeholders to identify and document shared redress processes and to clarify roles and responsibilities, consistent with relevant GAO guidance for coordination and documentation of internal controls.[14] In addition, Secure Flight, TSA OTSR, and TSA's Office of Intelligence (OI) have jointly produced guidance that clarifies how the entities will coordinate their respective roles in the redress process, consistent with GAO best practices on coordinating efforts across government stakeholders.[15] For example, the

[13]We have previously reported that the cleared list is not consistently used by air carriers, and that matched air travelers must still go to the airline ticket counter to provide information to confirm that they are the individual on the cleared list. See GAO, *Aviation Security: TSA Is Enhancing Its Oversight of Air Carrier Efforts to Identify Passengers on the No Fly and Selectee Lists, but Expects Ultimate Solution to Be Implementation of Secure Flight*, GAO-08-992 (Washington, D.C. Sept. 9, 2008).

[14]GAO, *Agency Performance Plans: Examples of Practices That Can Improve Usefulness to Decisionmakers*, GAO/GGD/AIMD-99-69 (Washington, D.C.: February 1999) and GAO/AIMD-00-21.3.1.

[15]See GAO/GGD/AIMD-99-69. TSA OI is responsible for disseminating the cleared list.

guidance clarifies the roles and responsibilities for each entity with respect to reviewing potential watch-list matches.

Furthermore, TSA is developing performance measures to monitor the timeliness and accuracy of Secure Flight redress, as we recommended in February 2008.[16] TRIP and OTSR's performance goals are to process redress applications as quickly and as accurately as possible. In February 2008, we reported that TRIP and OTSR track only one redress performance measure, related to the timeliness of case completion. We further reported that by not measuring all key defined program objectives, TRIP and OTSR lack the information needed to oversee the performance of the redress program. We recommended that DHS and TSA reevaluate the redress performance measures and consider creating and implementing additional measures, consistent with best practices that among other things address all program goals, to include the accuracy of the redress process.

In response to GAO's recommendation, representatives from the TRIP office are participating in a Redress Timeliness Working Group, with other agencies involved in the watch-list redress process, to develop additional timeliness measures. According to DHS officials, the TRIP office has also established a quality assurance review process to improve the accuracy of redress application processing and will collect and report on these data.

Secure Flight officials are developing additional performance measures to measure new processes that will be introduced once Secure Flight is operational, such as the efficacy of the system to preclear individuals who submit a redress number.

Condition 2: Minimizing False Positives

> Condition 2 requires that the underlying error rate of the government and private databases that will be used both to establish identity and assign a risk level to a passenger will not produce a large number of false-positives (mistakenly matched) that will result in a significant number of passengers being treated mistakenly or security resources being diverted.

TSA has generally achieved this condition by taking a range of actions that should minimize the number of false-positive matches. For example, the Secure Flight Final Rule requires air carriers to (1) collect date-of-birth information from airline passengers and (2) be capable of collecting

[16] See GAO-08-456T.

redress numbers from passengers.[17] Collecting date-of-birth information should improve the system's ability to correctly match passengers against watch-list records since each record contains a date of birth. TSA conducted a test in 2004 that concluded that the use of date-of-birth information would reduce the number of false-positive matches. In addition, airline passengers who have completed the redress process and are determined by DHS to not pose a threat to aviation security can submit their redress number when making a flight reservation. The submission of redress numbers by airline passengers should reduce the likelihood of passengers being mistakenly matched to watch list records, which in turn should reduce the overall number of false-positive matches.

TSA has established a performance measure and target for the system's false-positive rate, which should allow the agency to track the extent to which it is minimizing false-positive matches and whether the rate at any point in time is consistent with the program's goals. TSA officials stated that they tested the system's false-positive performance during Secure Flight's parallel testing with selected air carriers in January 2009 and found that the false-positive rate was consistent with the established target and program's goals.

Condition 3: Efficacy and Accuracy of the System and Stress Testing

Condition 3 requires TSA to demonstrate the efficacy and accuracy of the search tools used as part of Secure Flight and to perform stress testing on the Secure Flight system.[18]

We addressed efficacy and accuracy separately from stress testing because they require different activities and utilize different criteria.

Efficacy and Accuracy of the System

TSA has generally achieved the part of Condition 3 that requires TSA to demonstrate the efficacy and accuracy of the search tools used as part of Secure Flight. According to TSA, as a screening system, Secure Flight is

[17]The Secure Flight Final Rule provides that air carriers must request a passenger's full name, gender, date of birth, and Redress or Known Traveler Numbers (if available), but it only requires that passengers provide their full name, gender, and date of birth.

[18]Condition 3 also requires that TSA demonstrate that Secure Flight can make an accurate predictive assessment of those passengers who may constitute a threat to aviation. As TSA did not design Secure Flight with this capability, this element of the condition is not applicable to the Secure Flight program.

designed to identify subjects of watch-list records without generating an unacceptable number of false-positive matches.[19] To accomplish this goal, TSA officials stated that Secure Flight's matching system and related search parameters were designed to identify potential matches to watch-list records if a passenger's date of birth is within a defined range of the date of birth on a watch-list record.[20] According to TSA officials, the matching system and related search parameters were designed based on TSA OI policy and in consultation with TSA OI, the Federal Bureau of Investigation, and others.

TSA conducted a series of tests—using a simulated passenger list and a simulated watch list created by a contractor with expertise in watch-list matching—that jointly assessed the system's false-negative and false-positive performance. However, in conducting these tests, the contractor used a wider date-of-birth matching range than TSA used in designing the Secure Flight matching system, which the contractor determined was appropriate to test the capabilities of a name-matching system. The tests showed that the Secure Flight system did not identify all of the simulated watch-list records that the contractor identified as matches to the watch list (the false-negative rate).[21] Officials from TSA OI reviewed the test results and determined that the records not matched did not pose an unacceptable risk to aviation security.[22] These officials further stated that increasing the date-of-birth range would unacceptably increase the number of false positives generated by the system.

Moving forward, TSA is considering conducting periodic reviews of the Secure Flight system's matching capabilities and results (i.e., false

[19]TSA officials stated that they considered the Secure Flight program's objectives—for example, the system must process high volumes of passengers and quickly provide results to air carriers while also accounting for the TSA resources required to review potential matches—in determining an acceptable balance between mistakenly matching passengers (false-positives) and failing to identify passengers who match watch-list records (false-negatives).

[20]Details about the Secure Flight matching system and related search parameters are Sensitive Security Information and, therefore, are not included in this report. TSA designates certain information, such as information that would be detrimental to the security of transportation if publicly disclosed, as Sensitive Security Information pursuant to 49 U.S.C. § 114(r) and its implementing regulations, codified at 49 C.F.R. part 1520.

[21]Details about the specific false-negative rate resulting from these tests are Sensitive Security Information and, therefore, are not included in this report.

[22]See Appendix II for additional details about these tests.

positives and false negatives) to determine whether the system is performing as intended. However, final decisions regarding whether to conduct such reviews have not been made. Relevant guidance on internal controls identifies the importance of ongoing monitoring of programs, documenting control activities, and establishing performance measures to assess performance over time.[23] By periodically monitoring the system's matching criteria as well as documenting and measuring any results to either (1) confirm that the system is producing effective and accurate matching results or (2) modify the settings as needed, TSA would be able to better assess whether the system is performing as intended. Without such activities in place, TSA will not be able to assess the system's false-negative rate, which increases the risk of the system experiencing future performance shortfalls. Given the inverse relationship between false positives and false negatives—that is, an increase in one rate may lead to a decrease in the other rate—it is important to assess both rates concurrently to fully test the system's matching performance. In our January 2009 briefing, we recommended that TSA periodically assess the performance of the Secure Flight system's matching capabilities to determine whether the system is accurately matching watch-listed individuals while minimizing the number of false positives. TSA agreed with our recommendation.

Separate from the efficacy and accuracy of Secure Flight search tools, a security concern exists. Specifically, passengers could attempt to provide fraudulent information when making an airline reservation to avoid detection. TSA officials stated that they are aware of this situation and are taking actions to mitigate it. We did not assess TSA's progress in taking actions to address this issue or the effectiveness of TSA's efforts as part of this review. [24]

Stress Testing

The second part of Condition 3 requires TSA to perform stress testing on the Secure Flight system. In our January 2009 briefing to the Senate and House Appropriations Committees' Subcommittees on Homeland Security, we reported that TSA had generally not achieved this part of the condition because despite provisions for stress testing in Secure Flight test plans,

[23] See GAO/GGD/AIMD-99-69 and GAO/AIMD-00-21.3.1.

[24] Additional details on this issue were determined to be Sensitive Security Information by TSA and, therefore, are not included in this report.

such stress testing had not been performed at the time DHS certified that it had met the 10 statutory conditions, or prior to the completion of our audit work on December 8, 2008. However, TSA has since generally achieved this part of the condition.

According to the Secure Flight Test and Evaluation Master Plan, the system was to be stress tested in order to assess performance when abnormal or extreme conditions are encountered, such as during periods of diminished resources or an extremely high number of users. Further, the Secure Flight Performance, Stress, and Load Test Plan states that the system's performance, throughput, and capacity are to be stressed at a range beyond its defined performance parameters in order to find the operational bounds of the system.[25] In lieu of stress testing, program officials stated that Release 2 performance testing included "limit testing" to determine if the system could operate within the limits of expected peak loads (i.e., defined performance requirements).[26] According to the officials, this testing would provide a sufficient basis for predicting which system components would experience degraded performance and potential failure if these peak loads were exceeded. However, in our view, such "limit testing" does not constitute stress testing because it focuses on the system's ability to meet defined performance requirements only, and does not stress the system beyond the requirements. Moreover, this "limit testing" did not meet the provisions for stress testing in TSA's own Secure Flight test plans. Program officials agreed that the limit testing did not meet the provisions for stress testing in accordance with test plans and revised program test plans and procedures for Release 3 to include stress testing.

Beyond stress testing, our analysis at the time of our January 2009 briefing showed that TSA had not yet sufficiently conducted performance testing. According to the Secure Flight Test and Evaluation Master Plan, performance and load tests should be conducted to assess performance against varying operational conditions and configurations. Further, the Secure Flight Performance, Stress, and Load Test Plan states that each test

[25]Details about the specific stress test requirements are Sensitive Security Information and, therefore, are not included in this report.

[26]Performance tests are intended to determine how well a system meets specified performance requirements, while stress tests are intended to analyze system behavior under increasingly heavy workloads and severe operating conditions to identify points of system degradation and failure.

should begin within a limited scope and build up to longer runs with a greater scope, periodically recording system performance results. These tests also should be performed using simulated interfaces under real-world conditions and employ several pass/fail conditions, including overall throughput. However, Secure Flight Release 2 performance testing was limited in scope because it did not include 10 of the 14 Secure Flight performance requirements. According to program officials, these 10 requirements were not tested because they were to be tested as part of Release 3 testing that was scheduled for December 2008.[27] Moreover, 2 of the 10 untested performance requirements were directly relevant to stress testing. According to program officials, these 2 requirements were not tested as part of Release 2 because the subsystems supporting them were not ready at that time. Further, the performance testing only addressed the 4 requirements as isolated capabilities, and thus did not reflect real-world conditions and demands, such as each requirement's competing demands for system resources. Program officials agreed and stated that they planned to employ real world conditions in testing all performance requirements during Release 3 testing.

In our January 2009 briefing, we recommended that TSA execute performance and stress tests in accordance with recently developed plans and procedures and report any limitations in the scope of the tests performed and shortfalls in meeting requirements to its oversight board, the DHS Investment Review Board. Since then, based on our analysis of updated performance, stress, and load test procedures and results, we found that TSA has now completed performance testing and significantly stress tested the vetting system portion of Secure Flight. For example, the stress testing demonstrated that the vetting system can process more than 10 names in 4 seconds, which is the system's performance requirement. As a result of the performance and stress testing that TSA has recently conducted, we now consider this condition to be generally achieved and the related recommendation we made at our January 2009 briefing to be met.

[27]Our analysis showed that the Secure Flight Integrated Master Schedule (IMS) erroneously shows that performance testing for Release 3 was completed on July 31, 2008, which program officials confirmed was incorrect. According to program officials, the IMS was being updated to reflect its ongoing efforts to update and execute test plans in December 2008.

Condition 4: Establishment of an Internal Oversight Board

Condition 4 requires the Secretary of Homeland Security to establish an internal oversight board to monitor the manner in which the Secure Flight programs is being developed and prepared.

TSA has generally achieved this condition through the presence of five oversight entities that have met at key program intervals to monitor Secure Flight. In accordance with GAO's Standards for Internal Control in the Federal Government, a system of internal controls should include, among other things, an organizational structure that establishes appropriate lines of authority, a process that tracks agency performance against key objectives, and ongoing monitoring activities to ensure that recommendations made were addressed.[28] Consistent with these practices, the internal oversight entities monitoring the Secure Flight program have defined missions with established lines of authority, have met at key milestones to review program performance, and have made recommendations designed to strengthen Secure Flight's development. Our review of a selection of these recommendations showed that the Secure Flight program addressed these recommendations.

The oversight entities for the Secure Flight program are the following:

- DHS Steering Committee,
- TSA Executive Oversight Board,
- DHS Investment Review Board (IRB),[29]
- TSA IRB, and
- DHS Enterprise Architecture Board (EAB).

The DHS Steering Committee and TSA Executive Oversight Board are informal oversight entities that were established to provide oversight and guidance to the Secure Flight program, including in the areas of funding, and coordination with U.S. Customs and Border Protection (CBP) on technical issues. According to TSA officials, the DHS Steering Committee and TSA Executive Oversight Board do not have formalized approval requirements outlined in management directives. The DHS IRB, TSA IRB,

[28] GAO/AIMD-00-21.3.1.

[29] DHS Acquisition Directive 102-01 supersedes the previous investment review policy (Management Directive 1400). Under the new acquisition directive, issued in November 2008, the DHS Investment Review Board is now referred to as the Acquisition Review Board.

and DHS EAB are formal entities that oversee DHS information technology projects and focus on ensuring that investments directly support missions and meet schedule, budget, and operational objectives. (App. III contains additional information on these oversight boards.)

GAO has previously reported on oversight deficiencies related to the DHS IRB, such as the board's failure to conduct required departmental reviews of major DHS investments (including the failure to review and approve a key Secure Flight requirements document).[30] To address these deficiencies, GAO made a number of recommendations to DHS, such as ensuring that investment decisions are transparent and documented as required. DHS generally agreed with these recommendations. Moving forward, it will be critical for these oversight entities to actively monitor Secure Flight as it progresses through future phases of systems development and implementation and ensure that the recommendations we make in this report are addressed.

Conditions 5 and 6: Information Security

Conditions 5 and 6 require TSA to build in sufficient operational safeguards to reduce the opportunities for abuse, and to ensure substantial security measures are in place to protect the Secure Flight system from unauthorized access by hackers and other intruders.

TSA has generally achieved the statutory requirements related to systems information security based on, among other things, actions to mitigate high- and moderate-risk vulnerabilities associated with Release 3. As of completion of our initial audit work on December 8, 2008, which we reported on at our January 2009 briefing, we identified deficiencies in TSA's information security safeguards that increased the risk that the system will be vulnerable to abuse and unauthorized access from hackers and other intruders.

Federal law, standards, and guidance identify the need to address information security throughout the life cycle of information systems.[31]

[30]GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, GAO-09-29 (Washington, D.C.: Nov. 18, 2008) and GAO, *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, GAO-07-424 (Washington, D.C.: Apr. 27, 2007).

[31]We considered federal criteria including the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, §§ 301-05, 116 Stat. 2899, 2946-61 (as amended), OMB policies, and National Institute of Standards and Technology standards and guidelines.

Accordingly, the guidance and standards specify a minimum set of security steps needed to effectively incorporate security into a system during its development. These steps include

- categorizing system impact, performing a risk assessment, and determining security control requirements for the system;
- documenting security requirements and controls and ensuring that they are designed, developed, tested, and implemented;
- performing tests and evaluations to ensure controls are working properly and effectively, and implementing remedial action plans to mitigate identified weaknesses; and
- certifying and accrediting the information system prior to operation.[32]

To its credit, TSA had performed several of these key security steps for Release 1, such as:

- categorizing the system as high-impact, performing a risk assessment, and identifying and documenting the associated recommended security control requirements;
- preparing security documentation such as a system security plan and loading security requirements into the developer's requirements management tool;
- testing and evaluating security controls for the Secure Flight system and incorporating identified weaknesses in remedial action plans; and
- conducting security certification and accreditation activities.

However, as of December 8, 2008, TSA had not taken sufficient steps to ensure that operational safeguards and substantial security measures were fully implemented for Release 3 of Secure Flight. This is important because Release 3 is the version that is to be placed into production. Moreover, Release 3 provides for (1) a change in the Secure Flight operating environment from a single operational site with a "hot" backup site to dual processing sites where each site processes passenger data simultaneously,[33] and (2) the eSecure Flight Web portal, which provides an

[32]Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

[33]A hot site is a fully operation off-site data-processing facility equipped with hardware and system software to be used in the event of a disaster.

alternative means for air carriers to submit passenger data to Secure Flight. While these changes could expose the Secure Flight program to security risks not previously identified, TSA had not completed key security activities to address these risks.

Further, we found that TSA had not completed testing and evaluating of key security controls or performed disaster recovery tests for the Release 3 environment. These tests are important to ensure that the operational safeguards and security measures in the production version of the Secure Flight operating environment are effective, operate as intended, and appropriately mitigate risks. In addition, TSA had not updated or completed certain security documents for Release 3, such as its security plan, disaster recovery plan, security assessment report, and risk assessment, nor had it certified and accredited Release 3 of the Secure Flight environment it plans to put into production. Further, TSA had also not demonstrated that CBP had implemented adequate security controls over its hardware and software devices that interface with the Secure Flight system to ensure that Secure Flight data are not vulnerable to abuse and unauthorized access.

Finally, TSA had not corrected 6 of 38 high- and moderate-risk vulnerabilities identified in Release 1 of the Secure Flight program.[34] For example, TSA did not apply key security controls to its operating systems for the Secure Flight environment, which could then allow an attacker to view, change, or delete sensitive Secure Flight information. While TSA officials assert that they had mitigated 4 of the 6 uncorrected vulnerabilities, we determined the documentation provided was not sufficient to demonstrate that the vulnerabilities were mitigated. As a result of the security risks that existed as of December 8, 2008, we recommended that TSA take steps to complete its security testing and update key security documentation prior to initial operations.

After our January 2009 briefing, TSA provided documentation showing that it had implemented or was in the process of implementing our recommendation. For example, TSA had completed security testing of the most recent release of Secure Flight (Release 3), updated security

[34]TSA defines a vulnerability as high risk if the probability of serious incident is likely and the risk is not normally acceptable. According to TSA, there is a strong need for corrective action and the authorization of operation status may be rescinded or not granted. For moderate-risk vulnerability, the probability of an incident is elevated with increased probability of unauthorized disclosure or denial of service of critical systems.

documents, certified and accredited Release 3, received an updated certification and accreditation decision from CBP for its interface with the Secure Flight program, and mitigated the high- and moderate-risk vulnerabilities related to Release 1. In addition, TSA had prepared plans of actions and milestones (POA&M) for the 28 high-risk and 32 moderate-risk vulnerabilities it identified during security testing of Release 3. The POA&Ms stated that TSA would correct the high-risk vulnerabilities within 60 days and the moderate-risk vulnerabilities within 90 days. Based on these actions, we concluded that TSA had conditionally achieved this condition as of January 29, 2009.

Further, after we submitted our draft report to DHS for formal agency comment on March 20, 2009, TSA provided us updated information that demonstrated that it had completed the actions discussed above. Based on our review of documentation provided by TSA on March 31, 2009, we concluded that TSA had mitigated all 60 high- and moderate-risk vulnerabilities associated with Release 3. Therefore, we concluded that TSA had generally achieved the statutory requirements related to systems information security and we consider the related recommendation to be met.

Condition 7: Oversight of the Use and Operation of the System

Condition 7 requires TSA to adopt policies establishing effective oversight of the use and operation of the Secure Flight system.

As of the completion of our initial audit work on December 8, 2008, TSA had generally achieved this condition, but we nevertheless identified opportunities for strengthening oversight and thus made a recommendation aimed at doing so. According to GAO's best practices for internal control, effective oversight includes (1) the plans and procedures used to meet mission goals and objectives, and (2) activities that ensure the effectiveness and efficiency of operations, safeguard assets, prevent and detect errors and fraud, and provide reasonable assurance that a program is meeting its intended objectives.[35] To its credit, TSA had finalized the vast majority of key documents related to the effective oversight of the use and operation of the system as of the completion of our initial audit work on December 8, 2008. For example, TSA had established performance measures to monitor and assess the effectiveness of the Secure Flight program; provided training to air carriers on

[35]GAO/AIMD-00-21.3.1.

transitioning their watch-list matching functions to TSA; developed a plan to oversee air carriers' compliance with Secure Flight program requirements; and finalized key standard operating procedures. However, TSA had not yet finalized or updated all key program documents or completed necessary training, which was needed prior to the program beginning operations. Accordingly, we recommended that TSA finalize or update all key Secure Flight program documents—including the agreement with the Terrorist Screening Center for exchanging watch-list and passenger data and standard operating procedures—and complete training before the program begins operations. In response, TSA finalized its memorandum of understanding with the Terrorist Screening Center on December 30, 2008, and completed program training in January 2009. Based on these actions, we consider this recommendation to be met. Appendix IV contains additional information on Condition 7.

Condition 8: Privacy

Condition 8 requires TSA to take action to ensure that no specific privacy concerns remain with the technological architecture of the Secure Flight system.

TSA has generally achieved the statutory requirement related to privacy based on progress the agency has made in establishing a privacy program as well as recent actions taken to address security vulnerabilities related to conditions 5 and 6. In our January 2009 briefing, we identified deficiencies in TSA's information security safeguards that posed a risk to the confidentiality of the personally identifiable information maintained by the Secure Flight system.

The Fair Information Practices, a set of principles first proposed in 1973 by a U.S. government advisory committee, are used with some variation by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Australia, and New Zealand, as well as the European Union. The widely-adopted version developed by the Organisation for Economic Co-operation and Development in 1980 is shown in table 3.

Table 3: Fair Information Practice Principles

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organisation for Economic Co-operation and Development.

Note: A version of the Fair Information Practices, which has been widely adopted, was developed by the Organisation for Economic Co-operation and Development and published as Guidelines on the Protection of Privacy and Transborder Flow of Personal Data (Sept. 23, 1980).

At the time of our January 2009 briefing, TSA had established a variety of programmatic and technical controls for Secure Flight, including

- involving privacy experts in major aspects of Secure Flight development,
- developing privacy training for all Secure Flight staff and incident response procedures to address and contain privacy incidents,
- tracking privacy issues and performing analysis when significant privacy issues are identified,
- instituting access controls to ensure that data are not accidentally or maliciously altered or destroyed,
- filtering unauthorized data from incoming data to ensure collection is limited to predefined types of information,

- establishing standard formats for the transmission of personally identifiable information (PII) in order to reduce variance in data and improve data quality, and
- maintaining audit logs to track access to PII and document privacy incidents.

In addition, TSA had issued required privacy notices—including a Privacy Impact Assessment and System of Records Notice—that meet legal requirements and address key privacy principles. These notices describe, among other things, the information that will be collected from passengers and airlines, the purpose of collection, and planned uses of the data. Through its privacy program, TSA had taken actions to implement most Fair Information Practice Principles. For information on the actions TSA has taken to generally address Fair Information Practices, see appendix V.

However, at our January 2009 briefing, we also concluded that the weaknesses in Secure Flight's security posture—as described in our earlier discussion of information security—created an increased risk that the confidentiality of the personally identifiable information maintained by the Secure Flight system could be compromised. As a result, we recommended that TSA take steps to complete its security testing and update key security documentation prior to initial operations.

After our January 2009 briefing, TSA provided documentation that it had implemented or was in the process of implementing our recommendation related to information security and we concluded that this condition had been conditionally achieved as of January 29, 2009. Further, after we submitted our draft report to DHS for formal agency comment on March 20, 2009, TSA provided us updated information that demonstrated that it had completed the actions to implement our recommendation. Based on our review of documentation provided by TSA on March 31, 2009, we believe TSA has generally achieved the condition related to privacy.

Condition 9: CAPPS Rules

Condition 9 requires that TSA—pursuant to the requirements of section 44903(i)(2)(A)[sic] of title 49, United States Code—modify Secure Flight with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger primary selectee status.

TSA has generally achieved this condition. TSA is developing the Secure Flight program without incorporating the CAPPS rules and, therefore, Secure Flight will have no effect on CAPPS selection rates. According to TSA, the agency has modified the CAPPS rules to address air carriers operating in states with unique transportation needs and passengers who

might otherwise regularly trigger primary selectee status.[36] However, our review found that TSA lacked data on the effect of its modifications on air carrier selectee rates. We interviewed four air carriers to determine (1) the extent to which the CAPPS modifications and a related security amendment affected these carriers' selectee rates and (2) whether TSA had outreached to these carriers to assess the effect of the modifications and amendment on their selectee rates. The carriers provided mixed responses regarding whether the modifications and amendment affected their selectee rates. Further, three of the four air carriers stated that TSA had not contacted them to determine the effect of these initiatives. According to GAO best practices for internal control, agencies should ensure adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant effect on achieving goals.[37] Without communications with air carriers, and given the agency's lack of data on carrier selectee rates, TSA cannot ensure that the CAPPS modifications and related security amendment have their intended effect. In our January 2009 briefing, we recommended that TSA conduct outreach to air carriers—particularly carriers in states with unique transportation needs—to determine whether modifications to the CAPPS rules and security amendment have achieved their intended effect. TSA agreed with our recommendation.

TSA Has Conditionally Achieved 1 of the 10 Conditions, but Further Actions Are Needed to Mitigate the Risk of Cost and Schedule Overruns

Condition 10: Life-Cycle Cost and Schedule Estimates

> Condition 10 requires the existence of appropriate life-cycle cost estimates and expenditure and program plans.

TSA has conditionally achieved this statutory requirement based on our review of its plan of action for developing appropriate cost and schedule

[36]The CAPPS rules and TSA's actions in response to this condition are Sensitive Security Information and, therefore, are not included in this report.

[37]GAO/AIMD-00-21.3.1.

estimates and other associated documents submitted after we provided a copy our draft report to DHS for formal comment on March 20, 2009. The plan includes proposed activities and time frames for addressing weaknesses that we identified in the Secure Flight program's cost estimate and schedule and was the basis for our reassessment of this condition.

At the time of our January 2009 briefing, we reported that this condition had generally not been achieved. Specifically, while TSA had made improvements to its life-cycle cost estimate and schedule, neither were developed in accordance with key best practices outlined in our Cost Assessment Guide.[38] Our research has identified several practices that are the basis for effective program cost estimating. We have issued guidance that associates these practices with four characteristics of a reliable cost estimate: comprehensive, well documented, accurate, and credible. The Office of Management and Budget (OMB) endorsed our guidance as being sufficient for meeting most cost and schedule estimating requirements. In addition, the best practices outlined in our guide closely match DHS's own guidance for developing life-cycle cost estimates. Reliable cost and schedule estimates are critical to the success of a program, as they provide the basis for informed investment decision making, realistic budget formulation, program resourcing, meaningful progress measurement, proactive course correction, and accountability for results.

As we reported at our January 2009 briefing, Secure Flight's $1.36 billion Life Cycle Cost Estimate (LCCE) is well documented in that it clearly states the purpose, source, assumptions, and calculations. However, it is not comprehensive, fully accurate, or credible. As a result, the life-cycle cost estimate does not provide a meaningful baseline from which to track progress, hold TSA accountable, and provide a basis for sound investment decision making. In our January 2009 briefing, we recommended that DHS take actions to address these weaknesses. TSA agreed with our recommendation.

The success of any program depends in part on having a reliable schedule specifying when the program's set of work activities will occur, how long they will take, and how they relate to one another. As such, the schedule not only provides a road map for the systematic execution of a program, but it also provides the means by which to gauge progress, identify and

[38]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

address potential problems, and promote accountability. As we reported in January 2009, the November 15, 2008, TSA's Integrated Master Schedule (IMS) for Secure Flight—which provided supporting activities leading up to the program's initial operations in January 2009—was a significant improvement over its February 2008 version. For example, after meeting with GAO and its schedule analysis consultant, TSA took actions to improve the Secure Flight schedule, including adding initial efforts for domestic and international cutover activities, removing constraints that kept its schedule rigid, and providing significant status updates.

Our research has identified nine practices associated with effective schedule estimating, which we used to assess Secure Flight.[39] These practices are: capturing key activities, sequencing key activities, establishing duration of key activities, assigning resources to key activities, integrating key activities horizontally and vertically, establishing critical path, identifying float time, performing a schedule risk analysis, and distributing reserves to high risk activities.[40] In assessing the November 15, 2008, schedule against our best practices, we found that TSA had met one of the nine best practices, but five were only partially met and three were not met. Despite the improvements TSA made to its schedule for activities supporting initial operational capability, the remaining part of the schedule associated with implementing Secure Flight for domestic and international flights was represented as milestones rather than the detailed work required to meet milestones and events. As such, the schedule was more characteristic of a target deliverable plan than the work involved with TSA assuming the watch-list matching function. Moreover, likely program completion dates were not being driven by the schedule logic, but instead were being imposed by the program office in the form of target dates. This practice made it difficult for TSA to use the schedule to reflect the program's status. Without fully employing all key scheduling practices, TSA cannot assure a sufficiently reliable basis for estimating costs, measuring progress, and forecasting slippages. In our January 2009 briefing, we recommended that DHS take actions to address these weaknesses. TSA agreed with our recommendation.

[39]GAO-09-3SP.

[40]See app. VI for additional details on GAO's best practices for cost and schedule estimation.

In January 2009, TSA provided us with a new schedule, dated December 15, 2008. Our analysis showed that this new schedule continued to not follow best practices, did not correct the deficiencies we previously identified, and therefore could not be used as a reliable management tool. For example, a majority of the scheduled activities did not have baseline dates that allow the schedule to be tracked against a plan moving forward. In addition, best practices require that a schedule identify the longest duration path through the sequenced list of key activities—known as the schedule's critical path—where if any activity slips along this path, the entire program will be delayed. TSA's updated schedule did not include a critical path, which prevents the program from understanding the effect of any delays. Further, updating the Secure Flight program's schedule is important because of the significant cost and time that remains to be incurred to cutover all domestic flights to operations as planned by March 2010 and to develop, test, and deploy the functionality to assume watch-list matching for international flights.

After we submitted a copy of our draft report to DHS for formal agency comment on March 20, 2009, TSA provided us its plan of action, dated April 2009, that details the steps the Secure Flight program management office intends to carry out to address weaknesses that we identified in the program's cost and schedule estimates. With regard to the program's cost estimate, TSA's plan has established a timeline of activities that, if effectively implemented, should result in (1) a more detailed work breakdown structure that would define the work necessary to accomplish the program's objectives; (2) the cost estimate and schedule work breakdown structures being aligned properly; (3) an independent cost estimate performed by a contractor; (4) an assessment of the life-cycle cost estimate by the DHS Cost Analysis Division; and (5) cost uncertainty and sensitivity analyses. In addition, TSA's plan has estimated government costs that were originally missing from its cost estimate. According to TSA, these costs will be addressed in its life-cycle cost estimate documentation.

With regard to the Secure Flight program's schedule, TSA's plan of action has established a timeline of activities that, if effectively implemented, should result in, most notably: (1) a sequenced and logical schedule that will accurately calculate float time and a critical path; (2) a fully resource-loaded schedule based on subject-matter-expert opinion that does not overburden resources; (3) a schedule that includes realistic activity duration estimates; and (4) a schedule risk analysis that will be used by TSA leadership to distribute reserves to high-risk activities. According to TSA, this revised schedule will forecast the completion date for the project

based on logic, duration, and resource estimates rather than artificial date constraints.

The plan of action provides the Secure Flight program management office with a clearer understanding of the steps that need to be taken to address our concerns regarding the Secure Flight life-cycle cost estimate and schedule. Based on our review of the plan and the associated documentation provided, we therefore now consider this legislative requirement to be conditionally achieved and the related recommendations that we made at our January 2009 briefing to be met. It should be noted that a significant level of effort is involved in completing these activities, yet the actions—with the exception of the independent cost estimate—are planned to be completed by June 5, 2009. According to TSA, the independent cost estimate is to be completed by October 2009.

While TSA's ability to fully meet the requirements of Condition 10 does not affect the Secure Flight system's operational readiness, having reliable cost and schedule estimates allows for better insight into the management of program resources and time frames as the program is deployed. We will continue to assess TSA's progress in carrying out the plan of action to address the weaknesses that we identified in the program's cost estimate and schedule and fully satisfying this condition. Appendix VI contains additional information on our analysis of TSA's efforts relative to GAO's best practices.

Conclusions

TSA has made significant progress in developing the Secure Flight program, and the activities completed to date, as well planned, reduce the risks associated with implementing the program. However, TSA is still in the process of taking steps to address key activities related to testing the system's watch-list matching capability and cost and schedule estimates, which should be completed to mitigate risks and to strengthen the management of the program.

Until these activities are completed, TSA lacks adequate assurance that Secure Flight will fully achieve its desired purpose and operate as intended. Moreover, if these activities are not completed expeditiously, the program will be at an increased risk of cost, schedule, or performance shortfalls. Specifically, the system might not perform as intended in the future if its matching capabilities and results (that is, false positives and false negatives) are not periodically assessed. In addition, cost overruns and missed deadlines will likely occur if reliable benchmarks are not established for managing costs and the remaining schedule.

In addition to the issues and risks we identified related to the Secure Flight program, our work revealed one other TSA prescreening-related issue that should be addressed to mitigate risks and ensure that passenger prescreening is working as intended. Specifically, the effect that modifications to the CAPPS rules and a related security amendment have had on air carriers—particularly carriers in states with unique transportation needs—will remain largely unknown unless TSA conducts outreach to these air carriers to determine the effect of these changes.

Recommendations for Executive Action

We are recommending that the Secretary of Homeland Security take the following two actions:

- To mitigate future risks of performance shortfalls and strengthen management of the Secure Flight program moving forward, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration to periodically assess the performance of the Secure Flight system's matching capabilities and results to determine whether the system is accurately matching watch-listed individuals while minimizing the number of false positives—consistent with the goals of the program; document how this assessment will be conducted and how its results will be measured; and use these results to determine whether the system settings should be modified.

- To ensure that passenger prescreening is working as intended, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration to conduct outreach to air carriers—particularly carriers in states with unique transportation needs—to determine whether modifications to the CAPPS rules and related security amendment have achieved their intended effect.

Agency Comments and Our Evaluation

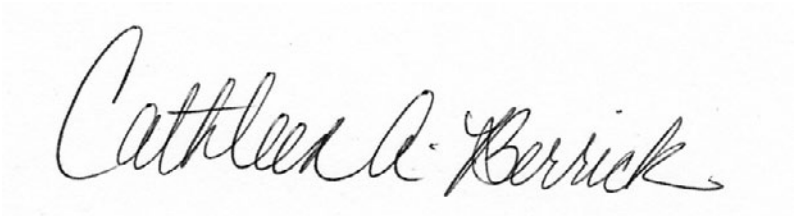
We provided a draft of this report to DHS for review and comment on March 20, 2009. Subsequently, TSA provided us additional information related to several of the conditions, which resulted in a reassessment of the status of these conditions. Specifically, in the draft report that we provided for agency comment, we had concluded that Conditions 5 and 6 (information security) and Condition 8 (privacy) were conditionally achieved and Condition 10 (cost and schedule) was generally not achieved. Based on our review of the additional documentation provided

by TSA, we are now concluding that Conditions 5, 6, and 8 are generally achieved and Condition 10 is conditionally achieved.

In addition, in the draft report we provided to DHS for agency comment, we made five recommendations, four of which were related to the Secure Flight program. The fifth recommendation was related to Condition 9 (CAPPS rules), which is not related to the Secure Flight program. Based on the additional information that TSA provided during the agency comment period, we now consider three of these recommendations to be met (those related to information security, the cost estimate, and the program schedule). The other two recommendations have not been met and, therefore, are still included in this report (those related to monitoring the performance of the system's matching capability and assessing the effect of modifications on CAPPS rules). We provided our updated assessment to DHS and on April 23, 2009, DHS provided us written comments, which are presented in appendix VII. In its comments, DHS stated that TSA concurred with our updated assessment.

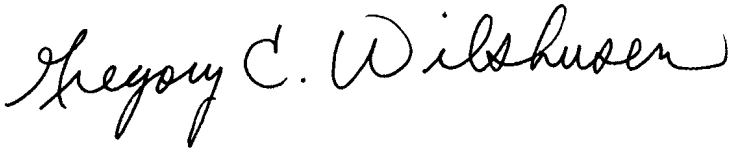
We are sending copies of this report to the appropriate congressional committees and other interested parties. We are also sending a copy to the Secretary of Homeland Security. This report will also be available at no charge on our Web site at http://www.gao.gov. Should you or your staff have any questions about this report, please contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov; Randolph C. Hite at (202) 512-3439 or hiter@gao.gov; or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are acknowledged in appendix VIII.



Cathleen A. Berrick
Managing Director, Homeland Security
and Justice Issues

Randolph C. Hite
Director, Information Technology
Architecture and Systems Issues



Gregory C. Wilshusen
Director, Information Security Issues

List of Congressional Committees

The Honorable Daniel K. Inouye
Chairman
The Honorable Thad Cochran
Vice Chairman
Committee on Appropriations
United States Senate

The Honorable John D. Rockefeller, IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United State Senate

The Honorable Patrick J. Leahy
Chairman
The Honorable Jeff Sessions
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Robert C. Byrd
Chairman
The Honorable George Voinovich
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable David R. Obey
Chairman
The Honorable Jerry Lewis
Ranking Member
Committee on Appropriations
House of Representatives

The Honorable Bennie G. Thompson
Chairman
The Honorable Peter T. King
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Edolphus Towns
Chairman
The Honorable Darrell Issa
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable James L. Oberstar
Chairman
The Honorable John L. Mica
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable David E. Price
Chairman
The Honorable Harold Rogers
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Objectives

In accordance with section 513 of the Department of Homeland Security Appropriations Act, 2008, our objective was to assess the extent to which the Transportation Security Administration (TSA) met the requirements of 10 statutory conditions related to the development and implementation of the Secure Flight program and the associated risks of any shortfalls in meeting the requirements.[1] Specifically, the act requires the Secretary of Homeland Security to certify, and GAO to report, that the 10 statutory conditions have been successfully met before TSA implements or deploys the program on other than a test basis.[2] Pursuant to the act, after the Department of Homeland Security (DHS) certified that it had satisfied all 10 conditions—which it did on September 24, 2008—we were required to report within 90 days on whether the 10 conditions had been successfully met. It further requires GAO to report periodically thereafter until it determines that all 10 conditions have been successfully met.

Scope and Methodology

Our overall methodology included (1) identifying key activities related to each condition; (2) identifying federal guidance and related best practices, if applicable, that are relevant to successfully meeting each condition (e.g., GAO's Standards for Internal Control in the Federal Government);[3] (3) analyzing whether TSA has demonstrated through verifiable analysis and documentation, as well as oral explanation, that the guidance has been followed and best practices have been met; and (4) assessing the risks associated with not fully following applicable guidance and meeting best practices. Based on our assessment, we categorized each condition as generally achieved, conditionally achieved, or generally not achieved.

- Generally achieved—TSA has demonstrated that it completed all key activities related to the condition in accordance with applicable federal

[1]See Pub. L. No. 110-161, Div. E, § 513, 121 Stat. 1844, 2072 (2007); see also Pub. L. No. 110-329, Div. D, § 512, 122 Stat. 3574, 3682-83 (2008).

[2]Section 522(a) of the Department of Homeland Security Appropriations Act, 2005 (Pub. L. No. 108-334, 118 Stat., 1298, 1319 (2004)), sets forth these 10 conditions.

[3]See GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982, provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to the 1982 Act, the Office of Management and Budget (OMB) issued circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in OMB Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

guidelines and related best practices, which should reduce the risk of the program experiencing cost, schedule, or performance shortfalls.

- Conditionally achieved—TSA has demonstrated that it completed some key activities related to the condition in accordance with applicable federal guidelines and related best practices and has defined plans for completing remaining key activities that, if effectively implemented as planned, should result in reduced risk that the program will experience cost, schedule, or performance shortfalls.

- Generally not achieved—TSA has not demonstrated that it completed all key activities related to the condition in accordance with applicable federal guidelines and related best practices and does not have defined plans for completing the remaining activities, and the uncompleted activities result in an increased risk of the program experiencing cost, schedule, or performance shortfalls.

In conducting this review, we worked constructively with TSA officials. We provided TSA with our criteria for assessing each of the 10 conditions and periodically met with TSA officials to discuss TSA's progress and our observations. To meet our 90-day reporting requirement, we conducted audit work until December 8, 2008, which included assessing activities and documents that TSA completed after DHS certified that it had met the 10 conditions. We reported the initial results of our review to the mandated reporting committees in two restricted briefings, first on December 19, 2008, and then on January 7, 2009. Because we concluded that TSA had not successfully met all 10 conditions, we conducted additional work from January through April 2009, the results of which are also included in this report. Further, after we submitted a copy of our draft report to DHS for formal agency comment on March 20, 2009, TSA provided us additional information related to Conditions 5, 6, 8, and 10 which resulted in our reassessment of the status of these conditions. The report has been updated to include the additional information and reassessments.

Condition 1: Redress

To assess Condition 1 (redress), we interviewed program officials and reviewed and assessed agency documentation to determine how, once Secure Flight becomes operational, the DHS redress process will be coordinated with the Secure Flight program, based upon GAO best practices for coordination; as well as whether the process was documented, consistent with GAO best practices on documenting internal

controls.[4] We also reviewed performance measures for the Secure Flight redress process as well as TSA's progress in addressing a February 2008 GAO recommendation that DHS consider creating and implementing additional measures for its redress process.[5]

Condition 2: Minimizing False Positives

To assess Condition 2 (minimizing false positives), we interviewed program and TSA Office of Intelligence (OI) officials and reviewed and assessed Secure Flight performance objectives, tests, and other relevant documentation to determine the extent to which TSA's activities demonstrate that the Secure Flight system will minimize its false-positive rate. Additionally, we interviewed program and TSA OI officials and reviewed and assessed Secure Flight documentation to determine how the program established performance goals for its false-positive and false-negative rates. We also interviewed a representative from the contractor that designed a dataset that TSA used to test the efficacy and accuracy of Secure Flight's matching system to discuss the methodology of that dataset. Our engagement team, which included a social science analyst with extensive research methodology experience and engineers with extensive experience in systems testing, reviewed the test methodologies for the appropriateness and logical structure of their design and implementation, any data limitations, and the validity of the results. Our review focused on steps TSA is taking to reduce false-positive matches produced by Secure Flight's watch-list matching process, which is consistent with TSA's interpretation of the requirements of this condition. We did not review the Terrorist Screening Center's role in ensuring the quality of records in the Terrorist Screening Database (TSDB).[6]

[4]GAO, *Agency Performance Plans: Examples of Practices That Can Improve Usefulness to Decisionmakers*, GAO/GGD/AIMD-99-69.

[5]GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-456T (Washington, D.C. Feb. 28, 2008).

[6]We reported on the quality of watch-list records in October 2007 and the steps the Terrorist Screening Center is taking to improve their quality; see GAO, *Terrorist Watch List: Screening Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C. Oct. 11, 2007). The Department of Justice's Inspector General also reported on the quality of records in the terrorist screening database in June 2005 and September 2007.

Condition 3: Efficacy and Accuracy of the System and Stress Testing

To assess the first part of Condition 3 (efficacy and accuracy of the system), we interviewed program and TSA OI officials and reviewed and assessed Secure Flight performance objectives, tests, and other documentation that address the type and extent of testing and other activities that demonstrate that Secure Flight will minimize the number of false positives while not allowing an unacceptable number of false negatives. We also interviewed a representative from the contractor that designed a dataset that TSA used to test the efficacy and accuracy of Secure Flight's matching system to discuss the methodology of that dataset. Our engagement team, which included a social science analyst with extensive research methodology experience and engineers with extensive experience in systems testing, reviewed the test methodologies for the appropriateness and logical structure of their design and implementation and the validity of the results. However, we did not assess the appropriateness of TSA's definition of what should constitute a match to the watch list. We did not assess the accuracy of the system's predictive assessment, as this is no longer applicable to the Secure Flight program given the change in its mission scope compared to its predecessor program CAPPS II (i.e., Secure Flight only includes comparing passenger information to watch-list records whereas CAPPS II was to perform different analyses and access additional data, including data from commercial databases, to classify passengers according to their level of risk).

To assess the second part of Condition 3, stress testing, we reviewed Secure Flight documentation—including test plans, test procedures, and test results—and interviewed program officials to determine whether TSA has defined and managed system performance and stress requirements in a manner that is consistent with relevant guidance and standards.[7] We also determined whether the testing that was performed included testing the performance of Secure Flight search tools under increasingly heavy workloads, demands, and conditions to identify points of failure. For example, in January 2009, we met with the Secure Flight development team and a program official to observe test results related to the 14 Secure Flight performance and stress requirements. We walked through each of the 14 requirements and observed actual test scenarios and results.

[7]Software Engineering Institute, "A Framework for Software Product Line Practice, Version 5.0"; "Robustness Testing of Software-Intensive Systems: Explanation and Guide," CMU/SEI-2005-TN-015; and GAO, *Year 2000 Computing Crisis: A Testing Guide* GAO/AIMD-10.1.21 (Washington, D.C.: Nov. 1, 1998).

Condition 4: Establishment of an Internal Oversight Board

To assess Condition 4 (internal oversight), we interviewed DHS and TSA program officials and reviewed and analyzed documentation related to various DHS and TSA oversight boards—the DHS and TSA Investment Review Boards, the DHS Enterprise Architecture Board, the TSA Executive Oversight Board, and the DHS Steering Committee—to identify the types of oversight provided to the Secure Flight program. We also reviewed agency documentation to determine whether the oversight entities met as intended and, in accordance with GAO's Standards for Internal Control in the Federal Government,[8] the extent to which the Secure Flight program has addressed a selection of recommendations and action items made by the oversight bodies. We evaluated oversight activities related to key milestones in the development of the Secure Flight system.

Conditions 5 and 6: Information Security

To assess Conditions 5 and 6 (information security), we reviewed TSA's design of controls for systems supporting Secure Flight. Using federal law, standards, and guidelines on minimum security steps needed to effectively incorporate security into a system, we examined artifacts to assess how system impact was categorized, risk assessments were performed, security control requirements for the system were determined, and security requirements and controls were documented to ensure that they are designed, developed, tested, and implemented.[9] We also examined artifacts to determine whether TSA assessed that controls were working properly and effectively, implemented remedial action plans to mitigate identified weaknesses, and certified and accredited information systems prior to operation. We interviewed TSA, U.S. Customs and Border Protection, and other officials on the current status of systems supporting, and controls, over Secure Flight. In addition, we observed the hardware and software environments of systems supporting Secure Flight to determine the status of information security controls, as appropriate. We reassessed the status of Conditions 5 and 6 based on our review of documentation provided by TSA on March 31, 2009, showing that it had mitigated all high- and moderate-risk information security vulnerabilities associated with the Secure Flight program's Release 3.

[8]GAO/AIMD-00-21.3.1.

[9]We considered federal criteria including the Federal Information Security Management Act of 2002, Office of Management and Budget policies, and National Institute of Standards and Technology standards and guidelines.

Condition 7: Oversight of the Use and Operation of the System

In regard to Condition 7 (oversight of the system), for purposes of certification, TSA primarily defined effective oversight of the system in relation to information security. However, we assessed DHS's oversight activities against a broader set of internal controls for managing the program, as outlined in GAO's Standards for Internal Control in the Federal Government, to oversee the Secure Flight system during development and implementation. We interviewed Secure Flight program officials and reviewed agency documentation—including policies, standard operating procedures, and performance measures—to determine the extent to which policies and procedures addressed the management, use, and operation of the system. We also interviewed program officials at TSA's Office of Security Operations to determine how TSA intends to oversee internal and external compliance with system security, privacy requirements, and other functional requirements. We did not assess the quality of documentation provided by TSA. Our methodology for assessing information security is outlined under Conditions 5 and 6.

Condition 8: Privacy

To assess Condition 8 (privacy), we analyzed legally-required privacy documentation, including systems-of-record notices and privacy impact assessments, as well as interviewed Secure Flight and designated TSA privacy officials to determine the completeness of privacy safeguards. In addition, we assessed available systems development documentation to determine the extent to which privacy protections have been addressed based on the Fair Information Practices.[10] We also assessed whether key documentation had been finalized and key provisions, such as planned privacy protections, had been clearly determined. We reassessed the status of Condition 8 based on our review of documentation provided by TSA on March 31, 2009, showing that it had mitigated all high- and moderate-risk information security vulnerabilities associated with the Secure Flight program's Release 3.

Condition 9: CAPPS Rules

To assess Condition 9 (CAPPS rules), we reviewed TSA documentation to identify modifications to the CAPPS rules and a related security program amendment to address air carriers operating in states with unique

[10]The version of the Fair Information Practices that we used, which has been widely adopted, was developed by the Organisation for Economic Co-operation and Development and published as *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980).

transportation needs and passengers who might otherwise regularly trigger primary selectee status. In addition, we interviewed TSA officials to determine the extent to which TSA assessed the effect of these activities on air carriers' selectee rates—either through conducting tests or by communicating with and obtaining information from air carriers—in accordance with GAO best practices for coordinating with external stakeholders.[11] We also interviewed officials from four air carriers to obtain their views regarding the effect of CAPPS changes on the air carriers' selectee rates. These carriers were selected because they operate in states with unique transportation needs or have passengers who might otherwise regularly trigger primary selectee status as a result of CAPPS rules.

Condition 10: Life-Cycle Cost and Schedule Estimates

To assess Condition 10 (cost and schedule estimates), we reviewed the program's life-cycle cost estimate, integrated master schedule, and other relevant agency documentation against best practices, including GAO's Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs.[12] We also interviewed key program officials overseeing these activities and consulted with a scheduling expert to identify risks to the integrated master schedule. We reassessed the status of Condition 10, based on TSA's plan of action provided to us on April 3, 2009. The Plan of Action, dated April 2009, details the steps the Secure Flight program management office intends to carry out to address weaknesses that we identified in the program's cost and schedule estimates. Appendix VI contains additional information on our analysis of TSA's efforts relative to GAO's best practices.

We conducted this performance audit from May 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[11]GAO/AIMD-00-21.3.1.

[12]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

Appendix II: Details on TSA's Testing of the Efficacy and Accuracy of Secure Flight's Matching System (Condition 3)

The Transportation Security Administration (TSA) hired a contractor with expertise in matching systems to construct a dataset against which to test the Secure Flight matching system and assess the system's false-positive and false-negative performance. Given the inverse relationship between false positives and false negatives—that is, a decrease in one may lead to an increase in the other—it is important to assess both rates concurrently to fully test the system's matching performance. The contractor developed the dataset specifically for Secure Flight using name-matching software and expert review by analysts and linguists.

The dataset consisted of a passenger list and a watch list using name types that were consistent with those on the actual No-Fly and Selectee lists. Each record included a passenger name and date of birth. The passenger list consisted of about 12,000 records, of which nearly 1,500 were "seeded" records that represented matches to the simulated watch list.[1] According to the contractor, the seeded records were plausible variations to passenger names and dates of birth based on the contractor's analysis of real watch-list records.

The passenger list was run through Secure Flight's automated matching system to determine its ability to accurately match the passenger records against the simulated watch list. The system used name-matching criteria outlined in the TSA No-Fly List security directive,[2] and a defined date-of-birth matching criteria that TSA officials state was consistent with TSA Office of Intelligence policy.[3]

According to TSA, Secure Flight officials reviewed the test results to determine whether the system was accurately applying its matching criteria for passenger name and date of birth. TSA officials concluded that all matches and nonmatches made by the system were in accordance with

[1]The number of seeded records, which represented matches to the watch list, does not reflect the actual number of watch-list matches in a real-world setting.

[2]A security directive is a regulatory tool through which TSA may impose security measures on a regulated entity, in this case air carrier, generally in response to an immediate or imminent threat. The No-Fly list security directive—SD 1544-01-20F (Apr. 9, 2008) specifies the number of name variations that must be used by air carriers for current watch-list matching. The specific number of name variations required in the directive and the Secure Flight's name-matching capabilities are Sensitive Security Information and therefore, not included in this report.

[3]This defined range is Sensitive Security Information and, therefore, is not included in this report.

these criteria. The test results for the system's default matching rules showed that the system produced a number of false-negative matches—that is, of the passenger records deemed by the contractor to be matches to the watch list, Secure Flight did not match a number of those records.[4] TSA officials stated that the false-negative rate in the test was primarily due to the Secure Flight system's criteria for a date-of-birth match, which differed from the contractor's criteria.

TSA determined a criteria range for a date-of-birth match that was consistent with TSA Office of Intelligence policy. According to TSA officials, these matching criteria are consistent with Secure Flight's responsibilities as a screening program—that is, the system must process high passenger volumes and quickly provide results to air carriers—and that those responsibilities were considered when balancing the risk presented by the system's false-positive and false-negative rates. The contractor's date-of-birth criteria range, however, was wider than the range used by TSA, which the contractor stated was established based on expert analysis of an excerpt from the watch list.

According to TSA officials, officials from TSA's Office of Intelligence reviewed the test results and determined that the records identified as false negatives by the contractor— that is, the records that were matched by the contractor but not by the Secure Flight system—did not pose an unacceptable risk and should not have been flagged, and that these nonmatches were designated as such in accordance with Office of Intelligence policies and TSA's No Fly list security directive. These officials further stated that increasing the date-of-birth range would unacceptably increase the number of false positives generated by the system.

TSA officials stated that the Secure Flight system's matching setting could be reconfigured in the future to adjust the system's false-positive and false-negative matching results should the need arise—for example, due to relevant intelligence information or improvements in the system's matching software.

[4]Details about the specific false-negative rate resulting from these tests are Sensitive Security Information and, therefore, not included in this report.

Appendix III: Secure Flight's Oversight Entities (Condition 4)

Table 4 shows the entities responsible for overseeing the development of the Secure Flight program and a sample of activities that had been completed.

Table 4: Responsibilities of Secure Flight's Oversight Entities and Selected Oversight Actions, as of March 2009

Entity	Oversight responsibilities	Completed activities	Sample recommendation	Remaining activities
Department of Homeland Security (DHS) Steering Committee	Review Secure Flight's progress in achieving key milestones and address operational issues. Prepare Secure Flight for other oversight processes (e.g., DHS Investment Review Board (IRB) review).	Met quarterly since April 2007 to monitor Secure Flight's schedule, funding and implementation approach.	The committee recommended improvements to Secure Flight concerning program documentation, such as the Mission Needs Statement, Concept of Operations, and briefing materials.	Meet quarterly to monitor program.
Transportation Security Administration (TSA) Executive Oversight Board	Review policy-related issues and assess the program's progress in meeting milestones. Monitor key program activities related to funding and system testing. Ensure coordination with other agencies such as CBP.	Met at least quarterly starting in November 2007 to oversee system, schedule and budget performance.	The board recommended that Secure Flight improve coordination with CBP, which resulted in a weekly forum on technical issues.	Meet quarterly to oversee program.
DHS IRB	Review Secure Flight's investments and authorize the program to move through Key Decision Points (KDP): (1) Program Initiation, (2) Concept and Technology Development, (3) Capability Development and Demonstration, (4) Production and Deployment, and (5) Operations and Support. Review and approve the program's Acquisition Program Baseline (APB) for cost, schedule, and performance.	Authorized Secure Flight to proceed through KDPs 1-3 and approved the APB.	Approved Secure Flight's progression to KDP 3 based on the program taking several actions including rescoping its business model to align more strongly with mission, which TSA addressed through a 60-day reassessment process.	Provide oversight for KDPs 4-5.
TSA IRB	Prepare Secure Flight to move through the KDPs governed by the DHS IRB and review and approve the system performance parameters delineated in the APB.	Met in conjunction with KDPs 1-3 and approved the APB.	Directed Secure Flight to coordinate program privacy and security compliance requirements with appropriate points of contact, which resulted in the updating of security and privacy documentation for the DHS IRB.	Provide guidance for KDPs 4-5.

Entity	Oversight responsibilities	Completed activities	Sample recommendation	Remaining activities
DHS EAB	Perform evaluations of Secure Flight to ensure the program is aligned with DHS enterprise architecture and technology strategies and capabilities. This occurs at the following Milestone Decision Points (MDP): (1) Project Authorization, (2) Alternative Selection, (3) Project Decision, (4) Pre-Deployment, and (5) Executive Review.	Authorized Secure Flight to move through MDP 1, 2, and 3.	Authorized Secure Flight to proceed through MDP 1 contingent on implementation of an Independent Verification and Validation capability, which TSA secured through a contract.	Provide oversight for MDP 4 and 5.

Source: GAO analysis.

Appendix IV: TSA's Activities Related to the Effective Oversight of System Use and Operation (Condition 7)

The Transportation Security Administration (TSA) completed several internal control activities related to the management, use, and operation of the Secure Flight system. For example:

- TSA developed 21 standard operating procedures related to Secure Flight's business processes. In addition, TSA incorporated additional programmatic procedures into various plans and manuals that will provide support for the program once it becomes operational. According to a Secure Flight official, all 21 standard operating procedures were finalized as of December 12, 2008.

- TSA released its Airline Operator Implementation Plan, which is a written procedure describing how and when an aircraft operator transmits passenger and nontraveler information to TSA. The plan amends an aircraft operator's Aircraft Operator Standard Security Program to incorporate the requirements of the Secure Flight program.

- TSA finalized its plan to oversee air carrier compliance with Secure Flight's policies and procedures. All domestic air carriers and foreign carriers covered under the Secure Flight rule will be required to comply with and implement requirements set forth in the final rule.

- The Airline Operator Implementation Plan and the Consolidated User Guide will provide air carriers with the requirements for compliance monitoring during the initial cutover phases.

- The Airline Implementation Team, which assists air carriers' transition to Secure Flight, will ensure that air carriers are in compliance with program requirements prior to cutover.

- TSA developed performance measures to monitor and assess the effectiveness of the Secure Flight program, such as measures to address privacy regulations, training requirements, data quality and submission requirements, and the functioning of the Secure Flight matching engine. TSA will also use performance measures to ensure that air carriers are complying with Secure Flight data requirements.

- TSA developed written guidance for managing Secure Flight's workforce, including a Comprehensive Training Plan that outlines training requirements for users and operators of the system and service centers.

- According to TSA officials, TSA completed programmatic training, which includes privacy and program-related training, for the entire Secure Flight workforce.

- TSA provided stakeholder training for covered U.S. air carriers and foreign air carriers on the Secure Flight program. This training, while not required of stakeholders, provided air carriers with information on changes to the Secure Flight program after the Final Rule was released and technical and operational guidance as outlined in the Consolidated User Guide. The Airline Implementation, Communications, and Training Teams will support requests from air carriers for additional training throughout deployment.

- According to TSA, the agency planned to pilot its operational training, which is necessary for employees and contractors to effectively undertake their assigned responsibilities, during the week of December 8, 2008. TSA officials stated that piloting this training would allow them to make any needed updates to Secure Flight's standard operating procedures. However, TSA officials said that updates to the Standard Operating Procedures as a result of training were expected to be minimal and would not have an effect on initial cutover in their view.

Appendix V: TSA's Actions to Address Fair Information Practices (Condition 8)

The Transportation Security Administration (TSA) has taken actions that generally address the following Fair Information Practices.

The Purpose Specification principle states that the purposes for a collection of personal information should be disclosed before collection and upon any change to that purpose. TSA addressed this principle by issuing privacy notices that define a specific purpose for the collection of passenger information. According to TSA privacy notices, the purpose of the Secure Flight Program is to identify and prevent known or suspected terrorists from boarding aircraft or accessing sterile areas of airports and better focus passenger and baggage screening efforts on persons likely to pose a threat to civil aviation, to facilitate the secure and efficient travel of the public while protecting individuals' privacy.

The Data Quality principle states that personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose. TSA addressed this principle through its planned use of the Department of Homeland Security's (DHS) Traveler Redress Inquiry Program (TRIP), collecting information directly from passengers, and setting standard data formats. More specifically, TSA is planning to use DHS TRIP as a mechanism to correct erroneous data. TSA also believes that relying on passengers to provide their own name, date of birth, and gender will further help ensure the quality of the data collected. Moreover, TSA has developed a Consolidated User Guide that provides standard formats for air carriers to use when submitting passenger information to reduce variance and improve data quality. We reported previously that the consolidated terrorist watch list, elements of which are matched with passenger data to make Secure Flight screening decisions, has had data- quality issues.[1] However, this database is administered by the Terrorist Screening Center and is not overseen by TSA.

The Openness principle states that the public should be informed about privacy policies and practices, and that individuals should have a ready means of learning about the use of personal information. TSA addressed this principle by publishing and receiving comments on required privacy

[1]We reported on the quality of watch-list records in October 2007 and the steps the Terrorist Screening Center is taking to improve their quality; see GAO, *Terrorist Watch List: Screening Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C.: Oct. 11, 2007).

notices. TSA has issued a Final Rule, Privacy Impact Assessment, and System of Records Notice that discuss the purposes, uses, and protections for passenger data, and outline which data elements are to be collected and from whom. TSA obtained and responded to public comments on its planned measures for protecting the data a passenger is required to provide.

The Individual Participation principle states that individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights. TSA addressed this principle through its planned use of DHS TRIP and its Privacy Act access and correction process. As previously mentioned, TSA plans to use DHS TRIP in order to allow passengers to request correction of erroneous data. Passengers can also request access to the information that is maintained by Secure Flight through DHS's Privacy Act request process. As permitted by the Privacy Act, TSA has claimed exemptions from the Privacy Act that limit what information individuals can access about themselves. For example, individuals will not be permitted to view information concerning whether they are in the Terrorist Screening Database (TSDB). However, TSA has stated that it may waive certain exemptions when disclosure would not adversely affect law enforcement or national security.

The Use Limitation principle states that personal information should not be used for other than a specified purpose without consent of the individual or legal authority. TSA addressed this principle by identifying permitted disclosures of data and establishing mechanisms to ensure that disclosures are limited to those authorized. The Secure Flight system design requires that data owners initiate transfers of information, a provision that helps to assure that data is being used only for specified purposes. According to TSA privacy notices, the Secure Flight Records system is intended to be used to identify and protect against potential and actual threats to transportation security through watch-list matching against the No-Fly and Selectee components of the consolidated and integrated terrorist watch list known as the Terrorist Screening Database. TSA plans to allow other types of disclosures, as permitted by the Privacy Act. For example, TSA is permitted to share Secure Flight data with

- federal, state, local, tribal, territorial, foreign, or international agencies responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order regarding a violation or potential violation of civil or criminal law or regulation; and

- international and foreign governmental authorities in accordance with law and formal or informal international agreements.

The Collection Limitation principle states that the collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual. TSA addressed this principle by conducting a data-element analysis, developing a data retention schedule, and establishing technical controls to filter unauthorized data and purge data. TSA has performed a data element analysis to determine the least amount of personal information needed to perform effective automated matching of passengers with individuals on the watch list. As a result, TSA has limited collection by only requiring that passengers provide their full name, gender, and date of birth. In addition, TSA requires air carriers to request other specific information, such as a passenger's redress number, and to provide TSA with other specific information in the airline's possession, such as the passenger's passport information. TSA established a data-purging control to rid the system of data according to its data-retention schedule. Further, TSA established technical controls to filter unauthorized data to ensure that collection is limited to authorized data fields. TSA is also developing a data-retention schedule which was issued for public comment and is in accordance with the Terrorist Screening Center's National Archives and Records Administration (NARA)—-approved record-retention schedule for TSDB records.

The Accountability principle states that individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles. TSA addressed the Accountability principle by designating a program privacy officer and a team of privacy experts working on various aspects of the Secure Flight program, and by planning to establish several oversight mechanisms:

- TSA implemented a system for tracking privacy issues that arise throughout the development and use of Secure Flight, and TSA is conducting follow-up analysis of significant privacy issues and providing resolution strategies for management consideration.

- TSA developed privacy rules of behavior, which require that individuals handling personally identifiable information (PII) only use it for a stated purpose.

- TSA is planning to maintain audit logs of system and user events to provide oversight of system activities, such as access to PII and transfer of PII in or out of the system.

- TSA is planning to issue periodic privacy compliance reports, intended to track and aggregate privacy concerns or incidents, but it has not finalized the reporting process.

- TSA developed general privacy training for all Secure Flight staff and is developing role-based privacy training for employees handling PII.

While TSA has also taken steps related to the Security Safeguards principle, this principle had not been fully addressed at the time of our January 2009 briefing. The Security Safeguards principle states that personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure. TSA actions to address the Security Safeguards principle include planning to prevent unauthorized access to data stored in its system through technical controls including firewalls, intrusion detection, encryption, and other security methods. Although TSA had laid out a plan to protect the confidentiality of sensitive information through various security safeguards, our security review—discussed in more detail under conditions 5 and 6 on information security—identified weaknesses in Secure Flight's security posture that create an increased risk that the confidentiality of the personally identifiable information maintained by the Secure Flight system could be compromised. As a result of the security risks we identified and reported on at our January 2009 briefing, and their corresponding effect on privacy, we recommended that TSA take steps to complete its security testing and update key security documentation prior to initial operations. TSA agreed with our recommendation.

Since our January 2009 briefing, TSA provided documentation that it has implemented our recommendation related to information security. In light of these actions, we believe TSA has now generally achieved the condition related to privacy and we consider the related recommendation we made at the briefing to be met.

Appendix VI: GAO Analyses of Secure Flight's Life-Cycle Cost Estimate and Schedule against Best Practices (Condition 10)

After submitting a copy of our draft report to the Department of Homeland Security (DHS) for formal agency comment on March 20, 2009, the Transportation Security Administration (TSA) provided us its plan of action, dated April 2009, that details the steps the Secure Flight program management office intends to carry out to address weaknesses that we identified in the program's cost and schedule estimates. We reviewed TSA's plan and associated documentation and reassessed the program against our Cost and Schedule Best Practices. The following tables show our original assessment and reassessment of TSA's cost and schedule against our best practices.

Table 5 summarizes the results of our analysis relative to the four characteristics of a reliable cost estimate based on information provided by TSA as of March 20, 2009.

Table 5: GAO Analysis of Secure Flight Cost Estimate Compared to Best Practices for a Reliable Cost Estimate Based on Information Provided by TSA as of March 20, 2009

Best practice	Explanation	Satisfied?	GAO analysis
Comprehensive	The cost estimates should include both government and contractor costs over the program's full life cycle, from the inception of the program through design, development, deployment, and operation and maintenance to retirement. They should also provide an appropriate level of detail to ensure that cost elements are neither omitted nor double- counted and include documentation of all cost-influencing ground rules and assumptions.	Partially	TSA's Life Cycle Cost Estimate (LCCE) included more cost elements (e.g., airline implementation, facility leasing costs, etc.) than the estimate it presented to us in February 2008. However, we found that support costs by other TSA groups assisting with Secure Flight were omitted, which resulted in an underreported cost estimate. In addition, because the costs for airline implementation were at a summary level, we could not determine what costs TSA estimated for implementing their assumed watch-list matching function for domestic and international flights. As a result, we could not determine if all costs were captured.
Well documented	The cost estimates should have clearly defined purposes and be supported by documented descriptions of key program or system characteristics. Additionally, they should capture in writing such things as the source data used and their significance, the calculations performed and their results, and the rationale for choosing a particular estimating method. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against, their sources. The final cost estimate should be reviewed and accepted by management.	Yes	The cost estimate explicitly identified the primary methods, calculations, results, assumptions, and sources of the data used to generate each cost element. The estimate was based on the engineering build up method, using actual costs when available, and included detail regarding the basis of estimate, the underlying data, and support for the labor hours, labor rates, and material costs. The estimate was reviewed by TSA's Chief Financial Officer group who verified that the figures presented were consistent with DHS and OMB summary of spending documentation.

Best practice	Explanation	Satisfied?	GAO analysis
Accurate	The cost estimates should provide for results that are unbiased and should not be overly conservative or optimistic. In addition, the estimates should be updated regularly to reflect material changes in the program, and steps should be taken to minimize mathematical mistakes and their significance. Among other things, the estimate should be grounded in a historical record of cost estimating and actual experiences on comparable programs.	Partially	Our data checks showed that the estimates were accurate; however, because TSA omitted some costs, it underestimated the LCCE. We also found that the work plan in the Integrated Master Schedule (IMS) was not reflected in the cost estimate, making variances between estimated and actual costs difficult. For example, while TSA's Secure Flight schedule shows domestic cutovers to be carried out in 12 groups, the cost estimate is based on labor categories, hours, and rates at a summary level. Tracking variances at this high level will not promote accountability and TSA will lose the opportunity to collect valuable estimating data that could improve the accuracy of international cutover cost estimates.
Credible	The cost estimates should discuss any limitations in the analysis performed due to uncertainty surrounding data or assumptions. Further, the estimates' derivation should provide for varying any major assumptions and recalculating outcomes based on sensitivity analyses, and their associated risks/uncertainty should be disclosed. Also, the estimates should be verified based on cross-checks using other estimating methods and by comparing the results with independent cost estimates.	Partially	TSA performed independent government cost estimates (IGCE) for some cost elements including contract support efforts. However, TSA did not compare its LCCE to an independent cost estimate for the entire Secure Flight program and therefore cannot gauge its reasonableness. In addition, we found no evidence that TSA performed cross-checks to determine if other cost estimating techniques produced similar results. TSA also did not perform an uncertainty analysis to quantify the risk associated with domestic and international cutovers. Finally, the Secure Flight program lacks a reliable schedule baseline, which is a key component of a reliable cost estimate because it serves as a basis for future work to be performed.

Source: GAO analysis.

Table 6 summarizes the results of our reassessment of the Secure Flight program's cost estimate relative to the four characteristics of a reliable cost estimate based on information provided by TSA as of April 3, 2009.

Table 6: GAO Reassessment of Secure Flight Cost Estimate Compared to Best Practices for a Reliable Cost Estimate Based on Information Provided by TSA as of April 3, 2009

Best practice	Explanation	Satisfied?	GAO analysis
Comprehensive	The cost estimates should include both government and contractor costs over the program's full life cycle, from the inception of the program through design, development, deployment, and operation and maintenance to retirement. They should also provide an appropriate level of detail to ensure that cost elements are neither omitted nor double- counted and include documentation of all cost-influencing ground rules and assumptions.	Partially	The program management office has estimated additional support costs associated with the Secure Flight program. These are government support costs expected to be incurred by TSA over the 3-year estimated period. The support costs are minor and will be noted in the LCCE assumptions. In planning to fully meet the Accurate best practice, TSA is planning to update its work breakdown structure (WBS) to define in detail the work necessary to accomplish Secure Flight's program objectives. TSA's Plan of Action states that each Secure Flight WBS area will be broken out into at least three levels. This work will be completed by July 2009.

Best practice	Explanation	Satisfied?	GAO analysis
Well documented	The cost estimates should have clearly defined descriptions of key program or system characteristics. Additionally, they should capture in writing such things as the source data used and their significance, the calculations performed and their results, and the rationale for choosing a particular estimating method. Moreover, this information should be captured in such a way that the data used to derive the estimate can be traced back to, and verified against, their sources. The final cost estimate should be reviewed and accepted by management.	Yes	TSA has fully met this criterion and therefore has no Plan of Action for reevaluation.
Accurate	The cost estimates should provide for results that are unbiased and should not be overly conservative or optimistic. In addition, the estimates should be updated regularly to reflect material changes in the program, and steps should be taken to minimize mathematical mistakes and their significance. Among other things, the estimate should be grounded in a historical record of cost estimating and actual experiences on comparable programs.	Partially	As noted in the Comprehensive best practice, the program management office has estimated additional support costs associated with the Secure Flight program. These are minor costs that will be noted in the LCCE assumptions. TSA's Plan of Action includes effort to fully align its cost estimate with the schedule WBS. TSA's Plan of Action also states that each Secure Flight WBS area will be broken out into at least three levels. A consistent framework between the IMS and cost estimate will promote accountability and will improve the accuracy of the cost estimate through the ability to track variances at lower levels. This work will be completed by July 2009.
Credible	The cost estimates should discuss any limitations in the analysis performed due to uncertainty surrounding data or assumptions. Further, the estimates' derivation should provide for varying any major assumptions and recalculating outcomes based on sensitivity analyses, and their associated risks/uncertainty should be disclosed. Also, the estimates should be verified based on cross-checks using other estimating methods and by comparing the results with independent cost estimates.	Partially	TSA's Plan of Action includes effort to use engineering build-up estimating techniques for each WBS work package, to be completed by July 2009. TSA will schedule an independent cost estimate (ICE) to be completed by a contractor by October 2009. In accordance with DHS directives, the DHS Cost Analysis Division will perform an assessment of the Secure Flight LCCE by April 2009. The ICE will be used to assess the reasonableness of the program office estimate and will be completed by April 2009. The Plan also includes effort to conduct a statistically based cost risk analysis. A Monte Carlo analysis will determine potential cost outcomes and will include a sensitivity analysis to identify key cost drivers. This uncertainty and sensitivity analysis will leverage results from the ICE effort and will be completed by May 2009.

Source: GAO analysis.

Table 7 summarizes the results of our analysis relative to the nine schedule-estimating best practices based on information provided by TSA as of March 20, 2009.

Table 7: GAO Analysis of Secure Flight Schedule Compared to Best Practices for Schedule Estimating Based on Information Provided by TSA as of March 20, 2009

Best Practice	Explanation	Satisfied?	GAO Analysis
Capturing key activities	The schedule should reflect all key activities as defined in the program's work breakdown structure (WBS), to include activities to be performed by both the government and its contractors.	Partially	TSA only identified at a summary level key activities associated with domestic and international airline operator cutovers even though a significant amount of uncertainty exists within this work. Without these data it will be difficult to estimate the true completion of the project. The schedule also did not include a project completion date activity which was necessary for conducting a schedule risk analysis.
Sequencing key activities	The schedule should be planned so that it can meet critical program dates. To meet this objective, key activities need to be logically sequenced in the order that they are to be carried out. In particular, activities that must finish prior to the start of other activities (i.e., predecessor activities), as well as activities that cannot begin until other activities are completed (i.e., successor activities), should be identified. By doing so, interdependencies among activities that collectively lead to the accomplishment of events or milestones can be established and used as a basis for guiding work and measuring progress.	Partially	There were some key missing logic links in the schedule and we found excessive and questionable use of nonstandard logic for sequencing activities. The schedule also contained little information regarding historical performance and lacked a reasonable representation of the work to be carried out, especially future effort related to domestic and international cutovers. As a result, the schedule was not adequate for planning, tracking, and maintaining detailed project control. TSA said it was challenging to tie four disparate schedules into a single IMS.
Establishing the duration of key activities	The schedule should realistically reflect how long each activity will take to execute. In determining the duration of each activity, the same rationale, historical data, and assumptions used for cost estimating should be used. Durations should be as short as possible and have specific start and end dates. Excessively long periods needed to execute an activity should prompt further decomposition so that shorter execution durations will result. The schedule should be continually monitored to determine when forecasted completion dates differ from the planned dates, which can be used to determine whether schedule variances will affect downstream work.	Partially	TSA's schedule showed that activity durations were hidden in lags rather than being identified in discrete activities that can be statused and monitored for progress. Many activities were represented as milestones instead of duration-driven tasks. Furthermore, rather than estimating remaining duration for activities, TSA overrode the finish date and the constraint type. This is not a standard scheduling practice and resulted in percent- complete errors and overly optimistic forecasting.
Assigning resources to key activities	The schedule should reflect what resources (e.g., labor, material, and overhead) are needed to do the work, whether all required resources will be available when needed, and whether any funding or time constraints exist.	No	TSA did not see the value in resource loading their schedule even though cost loading the schedule would provide an effective means of tracking cost overruns or underruns and keep the cost estimate updated in accordance with best practices.

Best Practice	Explanation	Satisfied?	GAO Analysis
Integrating key activities horizontally and vertically	The schedule is horizontally integrated, meaning that it linked the products and outcomes associated with already- sequenced activities. These links are commonly referred to as "handoffs" and serve to verify that activities are arranged in the right order to achieve aggregated products or outcomes. The schedule should also be vertically integrated, meaning that traceability exists among varying levels of activities and supporting tasks and subtasks. Such mapping or alignment among levels enables different groups to work to the same master schedule.	Yes	The majority of the schedule was both horizontally and vertically integrated, meaning that the activities across the multiple teams were arranged in the right order to achieve aggregated products or outcomes. In addition, traceability existed among varying levels of activities, which allowed multiple teams to work to the same master schedule.
Establishing the critical path for key activities	Using scheduling software, the critical path—the longest duration path through the sequenced list of key activities—should be identified. The establishment of a program's critical path is necessary for examining the effects of any activity slipping along this path. Potential problems that might occur along or near the critical path should also be identified and reflected in the scheduling of the time for high-risk activities.	Partially	TSA cannot completely identify the critical path because domestic and international cutover activities need to broken down into further detail, logic links need to be fixed, and activity durations need to be clearly identified. Furthermore, TSA's schedule for Secure Flight represented a "target-driven" schedule due to its high degree of milestones and target dates vs. dynamically calculated dates from the Microsoft Project software.
Identifying the "float time" between key activities	The schedule should identify float time—the time that a predecessor activity can slip before the delay affects successor activities—so that schedule flexibility can be determined. As a general rule, activities along the critical path typically have the least amount of float time. Total float describes the amount of time flexibility an activity has without delaying the project completion (if everything else goes according to plan). Total float is used to find out which activities or paths are crucial to project completion.	Partially	TSA identified float time in its schedule for some key activities it captured. However, this float was not a true indication of schedule flexibility because it was inflated due to the fact that many activities in the schedule had no successors. To fix the schedule, TSA would need to identify activity successors in order to properly identify float time.
Schedule risk analysis should be performed	A schedule risk analysis should be performed using statistical techniques to predict the level of confidence in meeting a program's completion date. This analysis focuses not only on critical path activities but also on activities near the critical path, since they can potentially affect program status.	No	TSA had not performed a schedule risk analysis. GAO conducted such an analysis in July 2008 and updated it in November 2008. GAO's schedule risk analysis was limited in its ability to account for risk due to the lack of detail provided by TSA for activities associated with domestic and international cutovers.
Distributing reserves to high risk activities	The baseline schedule should include a buffer or a reserve of extra time. Schedule reserve for contingencies should be calculated by performing a schedule risk analysis. As a general rule, the reserve should be applied to high-risk activities, which are typically found along the critical path.	No	Because TSA had not conducted its own Schedule Risk Analysis, it cannot identify appropriate schedule reserves.

Source: GAO analysis.

Table 8 summarizes the results of our reassessment of the Secure Flight program's schedule relative to the nine schedule estimating best practices based on information provided by TSA as of April 3, 2009.

Table 8: GAO Reassessment of Secure Flight Schedule Compared to Best Practices for Schedule Estimating Based on Information Provided by TSA as of April 3, 2009

Best practice	Explanation	Satisfied?	GAO analysis
Capturing key activities	The schedule should reflect all key activities as defined in the program's work breakdown structure, to include activities to be performed by both the government and its contractors.	Partially	In planning to fully meet the Accurate cost estimating best practice, TSA is planning to update its WBS to define in detail the work necessary to accomplish Secure Flight's program objectives. TSA's Plan states that each Secure Flight WBS area will be broken out into at least three levels. The estimated completion date for domestic deployment activities is April 2009 and June 2009 for international deployment activities.
Sequencing key activities	The schedule should be planned so that it can meet critical program dates. To meet this objective, key activities need to be logically sequenced in the order that they are to be carried out. In particular, activities that must finish prior to the start of other activities (i.e., predecessor activities), as well as activities that cannot begin until other activities are completed (i.e., successor activities), should be identified. By doing so, interdependencies among activities that collectively lead to the accomplishment of events or milestones can be established and used as a basis for guiding work and measuring progress.	Partially	As the schedule is updated to reflect domestic and international deployment activities, TSA is planning to "add dates and durations for key activities" that will be "supported by standard logic for sequencing activities." All detail tasks will have logical relationships in order for the scheduling software to dynamically calculate the completion date. This will allow the effect of actual and potential delays to be seen downstream. The plan further states that constraints and lags will be avoided and the schedule will have" accurate durations," but no mention is made of incorporating historical productivity. The estimated completion date for domestic deployment activities is April 2009 and June 2009 for international deployment activities.
Establishing the duration of key activities	The schedule should realistically reflect how long each activity will take to execute. In determining the duration of each activity, the same rationale, historical data, and assumptions used for cost estimating should be used. Durations should be as short as possible and have specific start and end dates. Excessively long periods needed to execute an activity should prompt further decomposition so that shorter execution durations will result. The schedule should be continually monitored to determine when forecasted completion dates differ from the planned dates, which can be used to determine whether schedule variances will affect downstream work.	Partially	According to the Plan of Action, constraints and lags will be avoided. The plan further states that the schedule will have "accurate durations," but no mention is made of incorporating historical productivity. However, based on GAO's recommendation, 1-day durations will operate off a 60-80 percent productivity day rather than the default 100 percent productive 8-hour day. These updates will be implemented as schedule activities are generated while the 1-day durations will be updated by April 24, 2009.

Best practice	Explanation	Satisfied?	GAO analysis
Assigning resources to key activities	The schedule should reflect what resources (e.g., labor, material, and overhead) are needed to do the work, whether all required resources will be available when needed, and whether any funding or time constraints exist.	No	According to the Plan of Action, the Secure Flight schedule is "completely resource loaded through domestic deployment." Resource loading was based on subject-matter-expert input and care was taken to ensure that resources were not overloaded. Resource loading is to be implemented as international deployment activities are generated, and completed by June 2009.
Integrating key activities horizontally and vertically	The schedule is horizontally integrated, meaning that it linked the products and outcomes associated with already sequenced activities. These links are commonly referred to as "handoffs" and serve to verify that activities are arranged in the right order to achieve aggregated products or outcomes. The schedule should also be vertically integrated, meaning that traceability exists among varying levels of activities and supporting tasks and subtasks. Such mapping or alignment among levels enables different groups to work to the same master schedule.	Yes	While this condition was originally met. TSA's Plan of Action guarantees that the updated schedule (including updated activities, durations, logic relationships, and resource loading) will continue to be horizontally and vertically integrated. The estimated completion date for domestic deployment activities is April 2009 and June 2009 for international deployment activities.
Establishing the critical path for key activities	Using scheduling software, the critical path—the longest duration path through the sequenced list of key activities—should be identified. The establishment of a program's critical path is necessary for examining the effects of any activity slipping along this path. Potential problems that might occur along or near the critical path should also be identified and reflected in the scheduling of the time for high-risk activities.	Partially	While not explicitly targeted in the Plan of Action, establishing the critical path is addressed through other scheduling efforts in the plan. In addition to updating the logic and incorporating realistic durations, the plan also states that dates will not be target-driven. In other words, the scheduling software will dictate a realistic finish date rather than the program office forcing tasks into the schedule to fit a predetermined date. The plan also notes that Level of Effort tasks will not show up in the critical path. This will be completed by June 2009.
Identifying the "float time" between key activities	The schedule should identify float time—the time that a predecessor activity can slip before the delay affects successor activities—so that schedule flexibility can be determined. As a general rule, activities along the critical path typically have the least amount of float time. Total float describes the amount of time flexibility an activity has without delaying the project completion (if everything else goes according to plan). Total float is used to find out which activities or paths are crucial to project completion.	Partially	As described previously, the Plan of Action calls for updating the logic relationships and incorporating realistic durations, as well as avoiding target –driven dates. Realistic float, as determined by the schedule, will then be available to the program office for resource leveling and schedule contingency. This will be implemented by April 2009 as international deployment activities are identified.

Best practice	Explanation	Satisfied?	GAO analysis
Schedule risk analysis should be performed	A schedule risk analysis should be performed using statistical techniques to predict the level of confidence in meeting a program's completion date. This analysis focuses not only on critical path activities but also on activities near the critical path, since they can potentially affect program status.	No	TSA has contracted with an independent company to (1) review the Secure Flight program plan, and (2) conduct and document a schedule risk analysis. The schedule risk analysis is to be completed by July 2009.
Distributing reserves to high risk activities	The baseline schedule should include a buffer or a reserve of extra time. Schedule reserve for contingencies should be calculated by performing a schedule risk analysis. As a general rule, the reserve should be applied to high-risk activities, which are typically found along the critical path.	No	According to the TSA Plan of Action, once the schedule risk analysis is completed, the results will be reviewed with program leadership to decide upon tasks that warrant reserves. This will be completed by August 2009.

Source: GAO analysis.

Appendix VII: Comments from the Department of Homeland Security

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

Homeland Security

April 23, 2009

Ms. Cathleen A. Berrick
Managing Director, Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20458

Dear Ms. Berrick:

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report titled, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks* (GAO-09-292).

GAO issued the aforementioned draft report to the Transportation Security Administration (TSA) on March 20, 2009. TSA noted that the information contained in the report concerning TSA's progress in achieving the statutory conditions was dated. Accordingly, between March 20, 2009 and April 10, 2009, TSA provided additional information and documentation to the GAO. As a result, the GAO advised TSA on April 13, 2009, that the Secure Flight program has generally achieved Conditions 1 through 9 and conditionally achieved Condition 10. TSA concurs with the updated GAO assessment.

The Department of Homeland Security through TSA will continue to collaborate with the GAO until Condition 10 has been generally achieved.

Sincerely,

Michael S. McPolland

for Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix VIII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen A. Berrick, (202) 512-3404 or berrickc@gao.gov

Randolph C. Hite, (202) 512-3439 or hiter@gao.gov

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Acknowledgments

In addition to the contacts listed above, Idris Adjerid, David Alexander, Mathew Bader, Timothy Boatwright, John de Ferrari, Katherine Davis, Eric Erdman, Anthony Fernandez, Ed Glagola, Richard Hung, Jeff Jensen, Neela Lakhmani, Jason Lee, Thomas Lombardi, Sara Margraf, Vernetta Marquis, Victoria Miller, Daniel Patterson, David Plocher, Karen Richey, Karl Seifert, Maria Stattel, Margaret Vo, and Charles Vrabel made key contributions to this report.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548