Department of Homeland Security

Office of Inspector General

Implementation and Coordination of TSA's Secure Flight Program

(Redacted)

OIG-12-94

July 2012

Table of Contents

Appendixes

Abbreviations

AIM	Airline Implementation Manager
BPPR	boarding pass printing result
CBP	U.S. Customs and Border Protection
CSA	Customer Service Agent
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
NCTC	National Counterterrorism Center
OI	Office of Intelligence
OIG	Office of Inspector General
OIT	Office of Information and Technology
SFA	Secure Flight Analyst
SFPD	Secure Flight Passenger Data
SOC	Secure Flight Operations Center
TIDE	Terrorist Identities Datamart Environment
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTAC	Transportation Threat Assessment and Credentialing
VID	verifying identity document
WLS	Watch List Service

Executive Summary

The Transportation Security Administration (TSA) is responsible for securing all modes of transportation, while also ensuring the freedom of movement for people and commerce. Through the Secure Flight program, TSA assumed from commercial aircraft operators the performance of passenger watch list matching for all covered flights into, out of, within, and over the United States. Aircraft operators are required to submit passenger data to Secure Flight prior to flight departure for advanced passenger prescreening.

We reviewed the Secure Flight program to determine whether it is screening all appropriate persons and whether the processes for aircraft operators to submit passenger data and receive boarding pass instructions are timely and effective. We also reviewed how the program's screening processes are tested for accuracy, prioritization, and timeliness, as well as how it is protecting personally identifiable and sensitive watch list information.

Government and private sector partners recognize the Secure Flight program's value, as it has provided more consistent passenger prescreening. [redacted] it has a defined system and processes to conduct watch list matching. To ensure that aircraft operators follow established procedures, Secure Flight monitors records and uses its discretion to forward issues for compliance investigation. Once Secure Flight assumed advanced passenger prescreening from aircraft operators, program focus shifted toward addressing emerging threats through multiple initiatives. We are making four recommendations to identify and eliminate system overrides, prioritize passenger data, standardize compliance, and improve communication and collaboration with partners. TSA concurred with Recommendations 1 and 3 and did not concur with Recommendations 2 and 4.

Background

Following the terrorist attacks of September 11, 2001, the U.S. Government needed to strengthen the security of the Nation's transportation systems, while also ensuring freedom of movement for people and commerce. The *Aviation and Transportation Security Act of 2001* established TSA, within the Department of Transportation, and tasked it with securing all modes of transportation, including commercial aviation.[1] As a result of the *Homeland Security Act of 2002*, in March 2003, TSA was transferred to the Department of Homeland Security (DHS) to unify the Nation's response to threats to the homeland.[2]

TSA issued security directives requiring commercial aircraft operators to perform passenger prescreening using the U.S. Government's consolidated terrorist watch list, known as the Terrorist Screening Database (TSDB), and matching passenger data against its No Fly and Selectee Lists. The No Fly List identifies individuals who are prohibited from boarding an aircraft or accessing the sterile area of a U.S. airport, while the Selectee List identifies individuals who are to receive additional physical screening prior to boarding an aircraft. Aircraft operators also conducted the same prescreening process for nontraveling persons authorized to enter sterile areas.[3]

In response to a recommendation in *The 9/11 Commission Report*,[4] the *Intelligence Reform and Terrorism Prevention Act of 2004*, as amended, directed TSA to develop an advanced passenger prescreening system and assume from aircraft operators the matching of passenger information to the No Fly and Selectee Lists, "utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government."[5] This act further required that TSA provide a redress process for misidentified individuals, limit the number of false positives, adopt policies establishing effective oversight, and implement security measures to protect the system

[1] 49 U.S.C. § 114 (a), (d).
[2] 6 U.S.C. § 203.
[3] The "sterile area" is the portion of an airport that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier, through the screening of persons and property. 49 CFR § 1540.5.
[4] *The 9/11 Commission Report*, p. 393.
[5] 49 U.S.C. § 44903(j)(2)(C)(i).

from unauthorized access and abuse.[6] When Congress transferred this responsibility to TSA, it required aircraft operators to supply TSA with passenger information needed to implement the advanced passenger prescreening system. Aircraft operators must also require third-party entities, such as travel agencies or booking websites, to provide passenger information to aircraft operators for submission to TSA.[7]

TSA developed the Secure Flight program to address federalizing commercial aircraft operator passenger prescreening. On October 28, 2008, TSA issued its Secure Flight Final Rule to implement the *Intelligence Reform and Terrorism Prevention Act of 2004* mandate requiring that TSA assume the passenger prescreening for domestic flights and international flights to, from, and overflying the United States.[8] Congress determined that advanced passenger prescreening should be a governmental function, and as a result, TSA, not commercial aircraft operators, bears the responsibility for conducting passenger prescreening.

The U.S. Government's Watchlisting System

To fulfill this responsibility, TSA uses various Federal Government databases to prescreen commercial aircraft passengers. Derogatory information for known or suspected terrorists is maintained in the National Counterterrorism Center's (NCTC) Terrorist Identities Datamart Environment (TIDE). Some information from this system and the Federal Bureau of Investigation (FBI) Automated Case Support system exports to the TSDB, which serves as the U.S. Government's consolidated terrorist watch list. The term "export" describes the transfer of record information from one database to another. From the TSDB, records meeting specific inclusion criteria export to the No Fly and Selectee Lists.

National Counterterrorism Center and the Terrorist Identities Datamart Environment

Within the Office of the Director of National Intelligence, the NCTC was established by Executive Order 13354 and the *Intelligence Reform and Terrorism*

[6] 49 U.S.C. § 44903(j)(2)(C)(iii).
[7] 49 U.S.C. § 44903(j)(2)(C)(iv)(II).
[8] Secure Flight Program; Final Rule, 73 Fed. Reg. 64018-64066 (Oct. 28, 2008).

Prevention Act of 2004 to implement a 9/11 Commission recommendation calling for the NCTC to serve as a center for joint operational planning and joint intelligence.[9] This act further directed that the NCTC will be the central and shared knowledge bank on known or suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. The NCTC is the primary U.S. Government organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government regarding terrorism and counterterrorism.[10] However, the tasks of collecting and analyzing intelligence pertaining exclusively to domestic terrorists, and investigating counterterrorism within the United States, fall primarily under the purview of the FBI.[11]

The NCTC is responsible for maintaining TIDE, the central repository of information on international terrorist identities. TIDE is a classified database that includes, to the extent permitted by law, all identifying and derogatory information that the U.S. Government possesses related to known or suspected terrorists. Homeland Security Presidential Directive-11 defines suspected terrorists as individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. Federal departments and agencies nominate individuals for inclusion in TIDE based on evaluations of intelligence and law enforcement terrorism information.

TIDE is the authoritative database on international known or suspected terrorists that supports the U.S. Government's watchlisting system. Homeland Security Presidential Directive-6 requires the NCTC to provide the Terrorist Screening Center (TSC) with access to all appropriate information or intelligence in its possession that the TSC needs to perform its functions.[12] As a result, the NCTC provides the TSC with a sensitive but unclassified subset of TIDE's international

[9] See *The 9/11 Commission Report*, p. 403.

[10] 50 U.S.C. § 404o(d)(1).

[11] See 28 U.S.C. §§ 509, 510, 533, and 534; 18 U.S.C. § 2332b(f); Executive Order 12333; 28 CFR § 0.85.

[12] Homeland Security Presidential Directive-6, *Integration and Use of Screening Information to Protect Against Terrorism*, September 16, 2003. The responsibilities of the Terrorist Threat Integration Center in this directive refer to responsibilities that have been assumed by the NCTC as of December 17, 2004, pursuant to the *Intelligence Reform and Terrorism Prevention Act of 2004*.

known or suspected terrorist identity information and access to TIDE Online, a read-only copy of the database.

Terrorist Screening Center and the Terrorist Screening Database

Homeland Security Presidential Directive-6 also instructed the U.S. Attorney General to establish an organization to consolidate the Government's approach to terrorism screening and to provide for the appropriate and lawful use of terrorist information in screening processes. To implement the directive, the Attorney General—acting through the Director of the FBI, and in coordination with the Secretary of State, Secretary of Homeland Security, and the Director of Central Intelligence—created the TSC.[13]

The TSC maintains the TSDB, which is populated with "information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism…."[14] All TSDB information is sensitive but unclassified, so the broadest range of Federal, State, local, and international terrorist screening partners can benefit from using data derived from the TSDB and exported by the TSC.

All TSDB information is derived from two sources. The only source for TSDB information on international terrorist identities is TIDE. The remaining information in the TSDB pertains solely to domestic terrorism information. This information is provided to the TSC directly from the FBI's Automated Case Support system, which contains additional supporting information on domestic terrorists, beyond any biometric and biographic identifiers exported to the TSDB.

There are minimum substantive derogatory and identifying criteria for inclusion in the TSDB. Although the NCTC accepts nominations that do not fully meet the TSDB derogatory and identifying criteria, it will enter those nominations into TIDE. The NCTC will not export that information to the TSC, however, unless both minimum criteria are met. After receiving TIDE information, the TSC

[13] *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism*, September 16, 2003.
[14] Homeland Security Presidential Directive-6.

reviews each nomination to ensure that it meets the U.S. Government's watchlisting standards before creating a TSDB record.

As part of its mission to maintain the U.S. Government's consolidated terrorist watch list, the TSC also exports data to other screening systems, including TECS. Some of these systems have their own minimum criteria or restrictions for inclusion, which may differ from TSDB requirements. TECS, which is owned and primarily used by U.S. Customs and Border Protection (CBP), accepts nearly all records from the TSDB and is used to screen individuals at land, sea, and air ports of entry. Many other Federal law enforcement departments and agencies also use TECS as a screening and case management system. The No Fly and Selectee Lists, which are subsets of the TSDB, have the most stringent substantive derogatory and identifying criteria and are used to identify individuals who are prohibited from boarding an aircraft or accessing the sterile area of a U.S. airport, or who are to receive additional physical screening prior to boarding.

No Fly and Selectee Lists

The No Fly and Selectee Lists' criteria were first established by the Homeland Security Council Deputies Committee on October 21, 2004. The Deputies Committee approved the addition of [redacted] criterion to the No Fly List on February 8, 2008. Following the attempted terrorist attack on December 25, 2009, the President directed that the No Fly and Selectee Lists' criteria be reviewed and recommendations be made as to whether any adjustments were needed. The TSC Policy Board Working Group, in conjunction with the Information Sharing Access Interagency Policy Committee, recommended certain changes in the lists' criteria and implementation guidance. Those recommendations were approved by the merged National Security Council/Homeland Security Council Deputies Committee on May 25, 2010.

For inclusion on either the No Fly or Selectee List, minimum identifying criteria consist of a first name, last name, and full date of birth. [redacted]

[redacted]

For inclusion on the No Fly List, an individual, regardless of citizenship, must represent—

- [redacted]

[redacted]

- [redacted]

[redacted] [redacted]

[redacted] [redacted]

The Selectee List is not a default list for individuals who do not qualify for inclusion on the No Fly List. Rather, the Selectee List includes persons, regardless of citizenship, in the TSDB who do not meet the criteria to be placed on the No Fly List and who are—

- [redacted]

[redacted] [redacted]

[redacted]

[redacted]

Secure Flight Program Implementation

When TSA issued the Secure Flight final rule in October 2008, it was allowed to begin implementing commercial aircraft operator passenger prescreening. Under this final rule, TSA receives specific passenger and nontraveler data and conducts watch list matching against the No Fly and Selectee Lists. A nontraveling individual or nontraveler refers to an individual to whom a covered aircraft operator or covered airport operator seeks to issue authorization to enter the sterile area. TSA then transmits a boarding pass printing result (BPPR) back to aircraft operators. This program is intended to provide consistent and accurate passenger prescreening, while minimizing false matches and protecting personally identifiable information.

Secure Flight Final Rule

The Secure Flight final rule covers all flights conducted by U.S. aircraft operators that are required to have a full program under 49 CFR § 1544.101(a),[21] and all

[redacted]

[21] 49 CFR § 1544 requires certain aircraft operators to adopt and carry out a security program approved by TSA, including screening procedures for passenger and property, threat response, and screener qualifications. Aircraft operators required to have a full security program under 49 CFR § 1544.101(a) are scheduled passenger or public charter passenger operations with an aircraft having a passenger seating

flights arriving in or departing from the United States or overflying the continental United States as operated by foreign aircraft operators that are required to have a security program under 49 CFR § 1546.101(a) or (b).[22] These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports.

With implementing the Secure Flight program, TSA requires covered aircraft operators to collect from passengers and transmit to TSA Secure Flight Passenger Data (SFPD). SFPD consists of a passenger's full name, gender, date of birth, and, when applicable, a Redress Number or Known Traveler Number. A Redress Number is a unique number that DHS assigns to individuals who use the DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP provides a single portal for travelers to seek redress for adverse screening experiences and to resolve possible watch list misidentification issues. A Known Traveler Number is a unique number assigned to "known travelers" for whom the Federal Government has already conducted a threat assessment and has determined do not pose a security threat.

According to the final rule, aircraft operators are required to make a privacy notice available on public websites and self-serve kiosks before collecting any personally identifiable information from passengers or nontravelers.[23]

The Secure Flight final rule also stipulates that aircraft operators must transmit available SFPD to TSA approximately 72 hours prior to the scheduled flight departure time. For reservations created within 72 hours of flight departure, aircraft operators must submit SFPD as soon as it becomes available. Secure Flight then matches the data provided against the No Fly and Selectee Lists. As

configuration of 61 or more seats, or 60 or fewer seats when passengers are enplaned from or deplaned into a sterile area.

[22] 49 CFR § 1546 applies to foreign air carriers permitted to operate in the United States and requires these carriers to adopt and carry out a security program approved by TSA, including the screening of passengers and property, and other requirements. Aircraft operators required to have a security program under 49 CFR § 1546.101(a) or (b) include (1) aircraft having a passenger seating configuration of 61 or more seats, or (2) operations that provide deplaned passengers access to a sterile area, or enplane passengers from a sterile area, when that access is not controlled by an aircraft operator using a security program under 49 CFR § 1544 or a foreign air carrier using a security program under 49 CFR § 1546.

[23] 49 CFR § 1560.103.

recommended by the 9/11 Commission and required by the *Intelligence Reform and Terrorism Prevention Act of 2004*, TSA "may use 'the larger set of watch lists maintained by the Federal government' when warranted by security considerations."[24] Based on TSA's matching results, Secure Flight instructs the covered aircraft operator in its BPPR to (1) process the individual in the normal manner; (2) identify the individual for additional screening at a security checkpoint; or (3) deny the individual boarding or authorization to enter a U.S. airport's sterile area.

[redacted] Secure Flight now screens all TSDB records that have full name and date of birth that are not already on the No Fly or Selectee Lists. These records compose the Expanded Selectee List; however, the Expanded Selectee List does not represent an official subset of the TSDB.

Secure Flight Program Organization

During our fieldwork, the Secure Flight program was positioned within TSA's Transportation Threat Assessment and Credentialing (TTAC). TTAC was the lead for all security threat assessments and credentialing initiatives for transportation industry workers, individuals seeking access to critical infrastructure, and domestic passengers. After our fieldwork ended in October 2011, TSA's realignment of headquarters functions merged TTAC vetting operations with its Office of Intelligence (OI) to form the new TSA Office of Intelligence and Analysis.

Within TTAC, Secure Flight was organized into the Secure Flight Operations Center (SOC) and Secure Flight program. The SOC was managed by the TTAC Vetting, Adjudication, and Redress program, and the Secure Flight program was under the TTAC Program Enrollment and Services Office. TTAC Technology managed the information technology support for TTAC, which included Secure Flight.

[24] Secure Flight Program; Final Rule, 73 Fed. Reg. 64018, 64019.

Secure Flight Operations Center

For the Secure Flight program, the SOC reviews and resolves potential watch list matches and answers general aircraft operator questions. Secure Flight has an Operations Support Desk to handle technical issues related to aircraft operators and internal Secure Flight operations. The Operations Support Desk provides aircraft operators, internal customers, and partners, such as the TSC and CBP, with a single point of contact and control for the resolution of technical incidents and problems.

Secure Flight's SOC has redundant operations in the Annapolis Junction Operations Center in Maryland and the Colorado Springs Operations Center in Colorado. The SOC operates 24 hours a day, 365 days a year. Centers are staffed with Government employees and contractors who serve as Customer Support Agents (CSAs), Secure Flight Analysts (SFAs), TSA OI Analysts, and Watch Managers. CSAs handle all initial calls received by the SOC, whether related to passenger resolution, customer support, or technical assistance. SFAs are responsible for matching SFPD to watch list records. TSA OI analysts are colocated with the SFAs and conduct threat and intelligence analysis, while assisting with the matching process. Watch Managers oversee both SOC locations to ensure that operations are performed properly and issues are addressed efficiently, effectively, and timely.

SOC employees are required to complete Secure Flight programmatic and operational training and on-the-job training. Programmatic training ensures that the workforces' knowledge aligns with program policies, procedures, and standards, while also improving critical competencies as defined by Secure Flight leadership. Examples of programmatic training include Introduction to the Aviation Industry and Secure Flight 101 courses. Operational training maintains and improves the readiness of employees and processes within the SOC. Examples of operational training include call handling and cultural naming courses to aid SOC employees with understanding various naming conventions and determining gender.

On-the-job training covers additional job-specific tasks and reinforces critical job-specific skills that are not fully covered in the programmatic or operational training. Employees are provided with a role-specific training checklist and are assigned to a trainer. Role-specific training checklists contain those job and mission-critical skills that the trainee is required to know and in which the trainee is required to demonstrate proficiency before being allowed to work unsupervised on Secure Flight systems.

Watch Managers are required to complete CSA and SFA certification, as well as Watch Manager training, as they may have to perform these duties at any time. Watch Managers complete their initial training at Annapolis Junction and finish their certification at their respective SOC.

Secure Flight Program Organization

The Secure Flight program consists of the following key offices: Business Architecture, Process, and Planning; Privacy; Industry Performance and Analysis; Change Management; and Program Management. In addition, TTAC Technology serves an important role in supporting Secure Flight systems.

<u>Business Architecture, Process, and Planning</u>

This office focuses on system transmissions, reengineering processes, and managing relationships with external offices within and outside of DHS, with the exception of the aircraft operators. The office is organized into three teams.

- <u>Team 1</u>: Works on issues related to receiving the watch list data, watch list matching, and Secure Flight responses to aircraft operators.

- <u>Team 2</u>: Works with scheduling Secure Flight system releases and requirements, production issues, and reports, such as those related to SFPD.

- <u>Team 3</u>: Works on security requirements and coordinates with CBP to ensure that technical and operational information is exchanged. These areas include testing aircraft operator SFPD transmissions, system outages, new requirements, and configuration changes.

Team personnel have additional responsibilities, such as project management for new system requirements, which can include defining system changes, conducting weekly meetings, or facilitating external partner collaboration and coordination.

The office also facilitates the Match Review Board and Match Review Working Group, which review the watch list matching process and identify ways to reduce "false positive" rates during passenger prescreening. A false positive is a passenger incorrectly identified as a potential match to an entry in the watch list. The Match Review Board and Match Review Working Group are quality control measures used by the Secure Flight program to ensure that the overall system performance is accurate and timely. Both provide a forum for regular review of Secure Flight match review procedures, to take corrective action or make recommendations for changes. They also review system-generated matching results regularly to identify problem areas or possible improvements, and provide those results to the Secure Flight program and TSA senior leadership for consideration.

Privacy Office

This office has helped to develop and implement a comprehensive privacy program to protect passenger personally identifiable information provided by aircraft operators. The Secure Flight privacy program aligns with TSA privacy principles, complies with industry best practices, and provides a defined redress process.

Industry Performance and Analysis

This office is composed of the Compliance Monitoring, Industry Performance, and Reporting and Analysis Groups. When the office is informed of a compliance issue, the Compliance Monitoring Group analyzes the issue and forwards a compliance package to TSA's Office of Security Operations or Office of Global Strategies to determine whether an investigation needs to be initiated. Airline Implementation Managers (AIMs) within the Industry Performance section liaise with aircraft operators on a daily basis to assist with issues, as needed. Reporting and Analysis is responsible for taking data from the SOC and creating reports, such as individual aircraft operator performance or response times, for the Secure Flight system.

TTAC Technology

This office develops information technology systems and maintains and operates all TTAC systems. TTAC Technology officials said that 70% of their work, which includes testing and deploying changes, involves the Secure Flight system.

Aircraft Operator Secure Flight Implementation Process

To allow watch list matching and admissibility determinations to be made before a flight departs to or from the United States, aircraft operators must be able to submit SFPD electronically to Secure Flight, and must also electronically submit passenger manifest information to CBP's Advance Passenger Information System.[25] The Advance Passenger Information System is an electronic data interchange system approved by CBP for air and vessel carrier transmissions of electronic passenger, non-crewmember (such as an animal handler on a cargo plane), and crewmember manifest data. The system processes biographical data from travelers, allowing it to be checked against law enforcement databases and watch lists. The Secure Flight final rule allowed for a phased implementation, in which TSA first assumed watch list matching responsibility for domestic flights. During this interim period, CBP prescreened international passengers against watch list systems and data subsets through the Advance Passenger Information System until Secure Flight was ready to begin watch list matching for all domestic and international passengers. CBP continues to screen international manifests through the Advance Passenger Information System.

To transmit data to DHS for both the Advance Passenger Information System and Secure Flight, aircraft operators must connect to and submit passenger data through a single DHS portal. This portal allowed DHS to integrate the watch list

[25] Aircraft manifests are lists of all passengers and crew on board a flight. Manifest information includes the full name, date of birth, gender, citizenship, country of residence, status on board the aircraft (i.e., passenger or crew member), DHS-approved travel document type, travel document number, travel document country of issuance, travel document expiration date, alien registration number (if applicable), and address while in the United States.

matching component of Secure Flight into the Advance Passenger Information System, thus streamlining the transmission of passenger information by aircraft operators.

Transition to Secure Flight and System Test Phases

Transitioning aircraft operators to implement Secure Flight has been a complex process of training, technical adjustments, and system testing, which continues, on a limited basis, for new aircraft operators. As a result, Secure Flight provides orientation training, technical support by phone, job aids, and training materials, as well as simulations to help aircraft operators comply with program requirements. Each aircraft operator designates an implementation point of contact, who communicates with Secure Flight AIMs and deployment teams. Teams include technical representatives who assist aircraft operators in completing required testing phases.

Secure Flight conducts testing in four phases: (1) aircraft operator internal system; (2) connectivity; (3) system-to-system interface; and (4) follow-on. Because aircraft operators are not required to update their existing systems to connect to Secure Flight, and because some systems are older, the process of transmitting and receiving data between older and newer systems is complex. As a result, system-to-system interface testing is an important phase. During this phase, aircraft operators are given data sets to transmit to Secure Flight through a test environment to ensure that all data are sent and can be read by the system, and that aircraft operators receive a proper BPPR from Secure Flight in return. During system-to-system interface testing and later through reporting tools, Secure Flight tests to ensure that it is receiving full passenger data.

Once aircraft operators complete a full range of system and operational testing, they can begin applying Secure Flight BPPR, which is referred to as the *cutover*. The first aircraft operator “domestic cutover” occurred on January 27, 2009. However, the first major aircraft operator domestic cutover occurred on November 5, 2009. Domestic carrier cutover was completed on June 22, 2010, and foreign carrier cutover was completed on November 23, 2010.

For aircraft operators with manual reservation systems, Secure Flight has an alternative to the DHS portal: a web application system called eSecure Flight. The system uses a secure user verification process to accept manually entered passenger information. Because the data for each passenger must be typed into the system, larger aircraft operators have generally modified their reservation and departure control systems to avoid manual data entry. As a result, eSecure Flight is typically used by smaller aircraft operators that have reservation systems with low volume. During our fieldwork, Secure Flight program officials said that 32 aircraft operators had cutover to eSecure Flight.

Secure Flight Program Partners

In addition to continuing partnerships with aircraft operators, the Secure Flight program collaborates and communicates with various DHS components and external departments and agencies that interact with aircraft operators or are involved in passenger prescreening and vetting.

Passenger Prescreening and Vetting

The TSC, for example, provides Secure Flight with an export of TSDB watch list records for passenger prescreening. Secure Flight receives TSDB watch list updates [redacted] and may receive expedited list updates at any time. The TSC has been working with CBP and TSA's Secure Flight program to implement the Department's Watch List Service (WLS), which will provide DHS with real-time access to continuously updated TSDB watch list records. Secure Flight uses these records to assess, vet, and determine potential passenger matches, which it forwards to the TSC for review and, as necessary, final identity match determination. Secure Flight can identify matches, but only the TSC has the authority to make final identity match determinations.

TSA OI analysts are colocated at both SOC locations, and provide subject matter expertise to SFAs to assist in confirming potential passenger matches to TSDB watch list records. When matches are identified, TSA OI analysts at Secure Flight contact the TSC for determinations on whether passenger matches are positive matches to TSDB watch list records. Once a determination is made, TSA OI communicates this information to the Intelligence Community and the TSA Freedom Center to execute operational response to the match.[26]

DHS TRIP is a multiagency effort designed to provide fair and timely redress, or remedy, to travelers who have difficulties with Federal Government screening and border crossing processes. DHS TRIP is the Federal Government's one-stop traveler redress process for coordinating the review, adjudication, and response to traveler redress requests. All travelers who apply through DHS TRIP receive a redress number. However, as DHS TRIP adjudicates all redress cases, only travelers who are not matches to TSDB watch list records are added to the DHS TRIP Cleared List. When purchasing tickets, all passengers may enter their redress number, but only passengers with redress numbers that match the DHS TRIP Cleared List are automatically cleared by the Secure Flight system. This process helps to prevent terrorists from determining their watch list status, even though they have a redress number. DHS TRIP provides [redacted] and then the list is provided to Secure Flight. DHS TRIP program officials said that they work with Secure Flight on traveler complaints.

CBP, through its National Targeting Center–Passenger, also screens international passengers. While Secure Flight screens all domestic and international passengers for matches against relevant TSDB watch list records, CBP screens all international passenger data for admissibility through several systems, including the Automated Targeting System–Passenger. The Automated Targeting System–Passenger develops risk assessments for each traveler based on rule sets that pertain to specific operational, tactical, or local enforcement objectives. The Automated Targeting System–Passenger provides records of passengers who have met the risk assessment threshold to Secure Flight for prescreening. Secure Flight uses this list to identify travelers requiring enhanced screening prior to boarding an aircraft. For international inbound passengers, the Secure Flight data is sent to CBP where it is screened against the Electronic System for Travel Authorization. The Electronic System for Travel Authorization is an Internet-based system used to determine, in advance of travel, the eligibility of

[26] The Freedom Center is TSA's coordination center during security incidents and operations. The center plays a critical role in in-flight and checkpoint security incidents, as well as coordination for every mode of transportation around the country and with law enforcement and security departments and agencies.

Visa Waiver Program applicants to travel to the United States. These travelers must apply for and receive an approved travel authorization via the system to board a plane or vessel bound for the United States.

In addition, CBP maintains the DHS Router system, which processes and converts aircraft operator data into SFPD for further processing by Secure Flight and CBP prior to retransmission to the aircraft operators. Further, CBP's Office of Information and Technology (OIT) will host the WLS on its servers.

Aircraft Operator Outreach

The Office of Transportation Sector Network Management and the Office of Global Strategies implement TSA's primary aircraft operator outreach programs, and often work with Secure Flight's Industry Performance and Analysis office. Program officials at Transportation Sector Network Management and the Office of Global Strategies are policy liaisons to aircraft operators, and receive from and provide information to operators and trade associations regarding TSA policy or regulatory changes. Both offices can communicate directly with aircraft operators for systemic problems, such as training issues, although the Office of Global Strategies is the primary liaison for foreign air carriers and international issues.

When SOC or Secure Flight program analysts notice irregular changes to SFPD information, Industry Performance and Analysis program officials create a compliance package. This package is forwarded to the Office of Global Strategies when activities involve foreign air carriers and U.S. aircraft operators operating in international locations. TSA's Office of Security Operations handles compliance issues for domestic flights. Both Offices of Security Operations and Global Strategies, however, conduct investigations concerning compliance issues based on their respective guidelines and authorities.

Secure Flight's operations require coordination with the Federal Aviation Administration (FAA), which controls aircraft within U.S. airspace. During some incidents, such as a No Fly passenger transiting U.S. airspace, a Selectee transiting U.S. airspace without proper screening [redacted] TSA requests the FAA's assistance in tracking passengers and controlling flights. When these incidents occur, Secure Flight notifies the Freedom Center, which communicates directly with the FAA. The FAA then tracks the flight and communicates with the aircraft's pilot-in-command to provide any additional instructions.

Through collaboration and coordination with internal and external partners, the Secure Flight program prescreens passengers to assist TSA in enhancing aviation security. We reviewed the Secure Flight program to determine whether it is screening all appropriate persons and whether the processes for aircraft operators to submit passenger data and receive boarding pass instructions are timely and effective. We also reviewed how the Secure Flight program tests its screening processes for accuracy, prioritization, and timeliness, as well as how the program is protecting varying layers of personally identifiable and sensitive watch list information.

Results of Review

[redacted] program officials monitor data transmissions to ensure that Secure Flight receives, prescreens, and vets all relevant passenger data. The program relies on aircraft operator compliance in submitting full and accurate passenger data, and SOC Watch Managers use their discretion to determine which issues are forwarded for further review or investigation.

Since Secure Flight has assumed responsibility for passenger prescreening from aircraft operators, the program has provided a more consistent watch list matching process. This process, however, is sometimes disrupted by DHS and airline system outages, which may require aircraft operators to revert to alternative procedures that may include pre-Secure Flight watch list matching procedures and protocols. To reduce disruptions, Secure Flight has operation center and system redundancy. Secure Flight also includes privacy safeguards to protect passenger personal data and sensitive watch list records and information. As the Secure Flight program's scope expands by developing and implementing additional initiatives, program officials should prioritize mission-critical elements first, and collaborate and communicate more effectively with relevant partners.

Secure Flight Relies on Passenger- and Aircraft Operator-Submitted Data and Aircraft Operator Compliance To Conduct Watch List Matching

The Secure Flight program relies on the accuracy of the information passengers submit during the reservation process. Aircraft operators submit this data to Secure Flight for watch list matching. Potential matches are manually reviewed, and unresolved matches require aircraft operator communication to the SOC for identity verification (see appendix D). According to Secure Flight program officials, more than 99% of passengers are cleared prior to arrival at an airport. Abnormalities, such as irregular changes to SFPD, are reported through a compliance process, but this process needs more standardization.

How Aircraft Operators Submit Passenger Data to Secure Flight

All passengers are required to provide their SFPD information to aircraft operators when making a reservation on a covered flight, and nontravelers must do so when they seek entry to an airport's sterile area. A passenger who refuses to provide these data elements is not permitted to board an aircraft or enter a sterile area. Aircraft operators can receive this data from any medium a passenger uses to make or modify a reservation (e.g., travel agency, Internet, self-service kiosks, gate locations). Aircraft operators are not required to validate the collected data during the reservation process.

Aircraft operators are also required to submit a passenger's passport number, expiration date, and country of issuance, if available, and certain non-personally identifiable information used to manage SFPD messages, such as the itinerary or the airport code for nontravelers. An aircraft operator stores this information in its automated reservation system or other passenger reservation or departure control system.

The aircraft operator transmits this information as an SFPD message, which can contain a new reservation record, modification of an existing record, or reservation cancellation. SFPD messages may also contain multiple passenger records. When the aircraft operator does not submit the passenger's full SFPD, the Secure Flight system will return an error message to the aircraft operator. Aircraft operators do not have to submit SFPD information for reservations canceled more than 72 hours prior to flight departure. Aircraft operators prioritize sending SFPD based on response time requirements and send SFPD via either a high-priority or low-priority queue. Data transmitted within 72 hours of departure are considered to be low priority, and data transmitted within 24 hours are considered high priority.

Although most aircraft operators use computerized reservation systems to store, retrieve, and submit passenger [redacted]

Secure Flight Vets Passenger Data Through an Automated Matching System

Secure Flight's watch list matching program is responsible for prescreening an average 2 million passengers every day. The program was implemented to enhance commercial air travel security, while providing an improved and consistent watch list matching system across all aircraft operators. Prior to Secure Flight implementation, TSA conducted a benchmark test to compare aircraft operator watch list matching rates to the initial Secure Flight automated matching system rates. TSA created [redacted] variations of names on the No Fly List and had aircraft operators and Secure Flight attempt to match them through their systems. The benchmark test determined that the average aircraft operator match rate was [redacted] aircraft operators tested, the operator that performed the best matched [redacted] of name variants, the worst matched [redacted] and Secure Flight matched [redacted] Secure Flight continually seeks to improve its vetting system and processes to achieve a 100% matching rate.

SFPD information is vetted through the Secure Flight automated matching system. This system performs automated matching of SFPD to various lists, including the No Fly, Selectee, and Expanded Selectee Lists, as well as the DHS TRIP Cleared List, CBP's Automated Targeting System–Passengers List, and the Centers for Disease Control and Prevention Do Not Board List.[27] An overwhelming majority of SFPD information is automatically cleared by the system, with an average 8.67-second system response time for low-priority records and 2.01-second average for high-priority records.

The Secure Flight automated matching system assigns a percentage score to each record, indicating the confidence level of a match between the passenger and the watch list entry. An exact match between SFPD information and watch list data elements produces a 100% match score; as the difference in data elements increases, the match score decreases. Scores must meet a minimum threshold to be considered a potential match and forwarded to an SFA for manual review; [redacted] which resulted in additional work. Increasing the threshold enables the Secure Flight program to vet more efficiently.

A cleared BPPR is transmitted from Secure Flight to aircraft operators when an individual's score is below the threshold, or is a potential match but is also a match to the DHS TRIP Cleared List. An automated Selectee BPPR is transmitted for any individual matching the Expanded Selectee List, the Automated Targeting System–Passengers List, or any passenger randomly selected for enhanced screening. For SFPD information that is a potential match to the No Fly, Selectee, or Do Not Board Lists, an inhibited BPPR response is returned to the aircraft operator and the SFPD is forwarded to an SFA for manual review.

[27] The Do Not Board List consists of individuals who pose a significant health risk to other travelers and are not allowed to fly.

In addition to matching original SFPD information, Secure Flight rematches SFPD submitted with qualified updates. An example of a qualified update is a change in any part of a passenger name or date of birth. Also, when records [redacted]

Potential Watch List Matches Are Sent to SFAs for Manual Match Review

SFPD matches to watch list records are updated and viewed electronically in the Secure Flight User Interface system, which prioritizes inhibited SFPD information in a queue according to flight departure times. SFAs log into and retrieve SFPD information through the Secure Flight User Interface queue to manually match passenger data against watch list records. SFAs use the automated matching result, passenger matching history, and the No Fly, Selectee, and DHS TRIP Cleared Lists as well as searches in TIDE Online and TECS for additional details, to discern whether the SFPD information is a match to the watch list record. SOC personnel retrieve records from the same Secure Flight User Interface queue, so a record is sent to the next available SFA regardless of the SFA's location.

SOC officials said the training [redacted] is helpful in conducting these searches, as SFAs can identify various [redacted] The Secure Flight system also applies a number of techniques to reduce false [redacted] SFAs are expected to vet a minimum [redacted] While this is not a requirement, such a measure is difficult to use when assessing an SFA's performance [redacted]

[redacted] SOC officials said this system change has resulted in reduced vetting times.

When an SFA is able to determine that SFPD information is not a match, a cleared BPPR is sent to the aircraft operator. When an SFA determines that a passenger is a match to the Selectee List, the SFA inhibits the record and contacts a TSA OI analyst, who prepares a preliminary Selectee notification report to alert the Intelligence Community and internal TSA organizations. When an SFA determines that a passenger is a match to the No Fly or Do Not Board List, the SFA retains the inhibited BPPR and contacts a TSA OI analyst, who generates a preliminary No Fly notification report. These preliminary notification reports allow Federal entities to coordinate coverage at airports and on aircraft, as necessary.

When an SFA cannot determine conclusively whether the passenger is a match to the No Fly, Selectee, or Do Not Board Lists using existing resources, the SFA retains the inhibited status and marks the record for further review. Through the resolution process, the aircraft operator will verify the passenger's identification to update the SFPD information and call the SOC should the passenger remain inhibited.

Aircraft Operators Call the SOC To Resolve Inhibited Passengers

An aircraft operator cannot print a passenger's boarding pass until it receives the appropriate BPPR from Secure Flight. When an aircraft operator receives an inhibited status, it must ask the passenger to provide a verifying identity document (VID) in person at the airport. A VID is an unexpired form of government-issued identification displaying the individual's full name, photo, and date of birth. An aircraft operator agent collects, verifies, and corrects, when necessary, the SFPD in the system using the information from the VID. After comparing the data, the agent updates the information as necessary and sends an updated SFPD submission to Secure Flight for re-matching, which is conducted in near real time. When the re-matching determines that the passenger is not a match, a cleared BPPR is sent to the aircraft operator. When the BPPR remains inhibited, the aircraft operator agent must call the SOC for resolution.

CSAs at the SOC receive resolution calls and authenticate a caller by collecting aircraft operator and airport codes. CSAs ask a series of questions to confirm that the aircraft operator has requested a VID and submitted any updates to Secure Flight. When the aircraft operator agent has not done so, CSAs explain the VID process. When the VID process has been completed, CSAs may ask, in coordination with SFAs, for additional information about the passenger, including the passenger's driver's license or passport number or a physical description. [redacted] CSAs enter this information into the Secure Flight User Interface and send the records to SFAs for matching.

SFAs use the additional information to vet potential matches and transmit the appropriate BPPR. [redacted] When a passenger appears to be a match to the No Fly or Do Not Board Lists, the current inhibited status is retained.

For positive matches, the SFA then notifies a TSA OI analyst, who generates an updated notification report and assists in resolution. TSA OI analysts have access to additional databases beyond TIDE Online and TECS that SFAs do not access. TSA OI analysts also work with the TSC to obtain a Final Identity Match Determination.

Secure Flight Is Addressing Challenges, But Some Vulnerabilities Remain

Federal Government and private sector partners recognize Secure Flight's value and have seen improvements since its initial implementation and cutover. Secure Flight has worked to address new and existing challenges, though some vulnerabilities remain.

The majority of aircraft operators we interviewed note a decrease in the average resolution call time since Secure Flight's implementation. The average call response time for FY 2011 was 7 seconds with most resolution calls lasting 2 to 8 minutes, but a CSA will stay on a call as long as necessary to resolve any issues.

One frustration aircraft operators voiced, however, is that when a transmitted BPPR is inhibited, they may spend 30 minutes or more on a resolution call, even though the CSA says the passenger is cleared. For example, this may occur when an original BPPR is initially marked inhibited but subsequently cleared, and then the passenger changes to an earlier flight. In this example, the BPPR requires revetting, during which the BPPR reverts to inhibited. Aircraft operator representatives said this occurs more during irregular operations, such as inclement weather events, when more passengers change flights. Some aircraft operators have overridden these inhibited BPPRs and printed a cleared boarding pass to keep passengers from missing flights.

Some aircraft operators we interviewed that experience this problem are told that it occurs because the inhibited record is delayed in the Secure Flight User Interface queue. Although Secure Flight officials said that this does not occur often, these inhibited BPPRs should be handled through the high-priority queue and therefore resolved quickly. In addition, an aircraft operator's ability to override inhibited BPPRs raises concern that some inhibited passengers are not being handled appropriately.

Recommendations

We recommend that the Director of the Secure Flight program:

Recommendation #1:

Identify how and when aircraft operators override an inhibited boarding pass printing result and implement corrective action to eliminate unauthorized overrides by aircraft operators.

Recommendation #2:

Ensure that aircraft operators prioritize Secure Flight passenger data appropriately and receive an accurate, updated boarding pass printing result when aircraft operators submit changes.

Management Comments and OIG Analysis

We evaluated TSA's written comments and have made changes to the report where we deemed appropriate. A summary of TSA's written response to the report recommendations and our analysis of the response follows each recommendation. A copy of TSA's response, in its entirety, is included as appendix C.

In addition, we received technical comments from TSA, CBP, and DHS' Office of Policy, as well as the FBI, and incorporated these comments into the report where appropriate. We also solicited comments from the FAA; however, the FAA did not have any technical changes to the draft report. TSA concurred with two recommendations and did not concur with two recommendations in the report. We appreciate the comments and contributions made by each entity.

Management Response: TSA officials concurred with Recommendation 1. In its response, TSA said that Secure Flight has always taken steps to identify how and when aircraft operators inappropriately override boarding pass printing results. When Secure Flight is able to identify cases of aircraft operators inappropriately overriding results, TSA takes steps to ensure that screening is performed, and to launch compliance investigations or responses. TSA said that it has been performing these actions since Secure Flight's operational start-up on January 27, 2009, and considers action complete on this recommendation.

OIG Analysis: We consider TSA's actions responsive to the intent of Recommendation 1, which is resolved and open. This recommendation will remain open pending the receipt of documentation demonstrating corrective actions taken and planned to eliminate unauthorized overrides by aircraft operators.

Management Response: TSA did not concur with Recommendation 2. In its response, TSA said that Secure Flight has provided prioritization queues for the aircraft operators' use since the inception of operations in 2009. It is, and has been, the obligation of the aircraft operators to submit passenger data to the appropriate (high or low) priority queue. This is, and has been, specified in guidance documentation provided to aircraft operators and is tested and operationally checked by Secure Flight.

TSA considers this to be an effective and efficient process to ensure the prioritization of passenger data and that Secure Flight is providing accurate and updated boarding pass printing results when aircraft operators submit changes to Secure Flight.

OIG Analysis: Although TSA did not concur with this recommendation, we consider the actions responsive to the intent of Recommendation 2, which is resolved and open. While TSA has provided guidance to aircraft operators on the submission of passenger data to the appropriate priority queue, issues were reported to us concerning aircraft operators' prioritization of records and receipt of accurate boarding pass printing instructions. This recommendation will remain open pending our receipt of information evidencing Secure Flight's collaboration with aircraft operators to (1) identify and remedy issues relating to the submission of data to the appropriate priority queue, and (2) identify and resolve inaccurate boarding pass printing results that aircraft operators receive following submitted changes.

Inhibited Boarding Pass Records Are Monitored To Ensure Aircraft Operator Compliance

Secure Flight does not know when an aircraft operator or passenger prints a boarding pass. However, because the program conducts automated and manual matching at least 24 hours prior to a flight's departure, SOC Watch Managers track inhibited records to ensure that aircraft operators complete the resolution process. To address this challenge, the SOC compiles a daily list of all the scheduled inhibited passengers and their itinerary information. The Watch Managers contact aircraft operators 30 to 45 minutes prior to flight departure for a status update when a scheduled inhibited passenger has not been resolved. When an inhibited passenger has incorrectly received a cleared boarding pass or has otherwise gained access to the sterile area or an aircraft, the SOC [redacted]

[redacted] has been successful and has not resulted in an increase in resolution calls or unfavorable comments from aircraft operators.

Aircraft Operators Are Adapting to Secure Flight Processes, But Concerns Remain Over the Accuracy of Passenger-Submitted Data

According to Secure Flight, the SOC receives an average of 114 calls daily and manually reviews an average of 39,279 SFPDs each week. As more than 200 aircraft operators are cutover to Secure Flight and approximately 2 million passengers fly each day, agents may not be handling inhibited passengers as often, and the VID and resolution processes are different from pre-Secure Flight aircraft operator operating procedures. In cutting over to Secure Flight, aircraft operator personnel needed to learn new processes and terminology, and had to adjust their systems to reflect these changes. In addition, more than 140 international aircraft operators are submitting SFPD information, and some communications between agents and the SOC present challenges.

[redacted] For example, one aircraft operator noted [redacted] This was confirmed in various Secure Flight incident reports.

Secure Flight Is One Aspect of TSA's Multilayered Security Approach

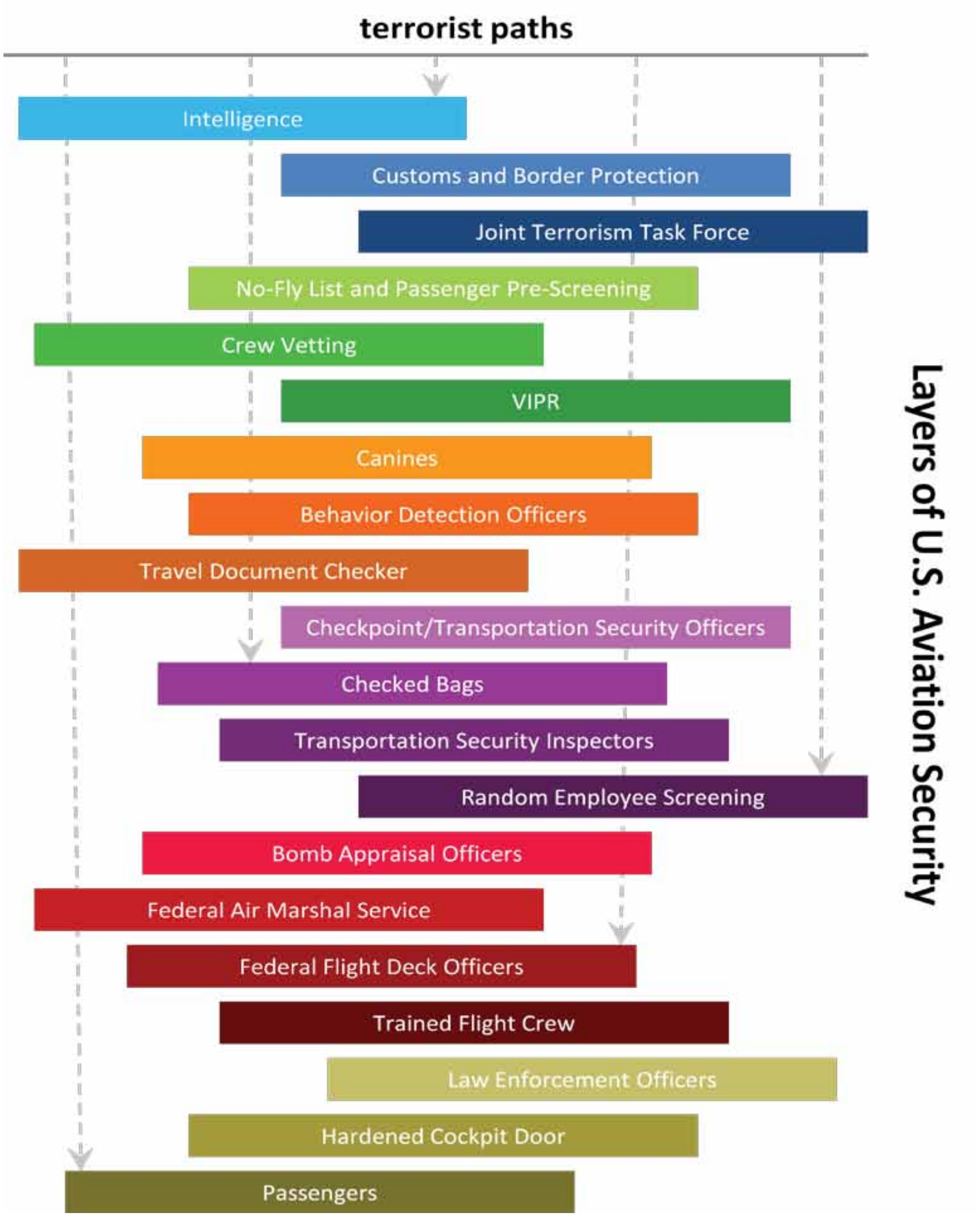
Although these vulnerabilities exist, TSA uses a multilayered approach to ensure the overall security of the traveling public and the Nation's transportation system (see figure 1). For example, Travel Document Checkers are specially trained TSA Transportation Security Officers who verify boarding passes and identification documents at airport checkpoints before allowing a traveler or nontraveler access to an airport's sterile area. On aircraft, Federal Air Marshals[28] and Federal Flight Deck Officers[29] provide another security layer. In addition to Secure Flight prescreening efforts, CBP's National Targeting Center–Passenger provides passenger vetting for international flights. [redacted] These partners work together to serve the larger mission of aviation security.

Figure 1 illustrates that an individual would have to overcome multiple security layers, irrespective of the path used, to breach aviation security; paths are represented by vertical dotted lines.

[28] Federal Air Marshals blend in with passengers and rely on their training, including investigative techniques, criminal terrorist behavior recognition, firearms proficiency, aircraft-specific tactics, and close quarters self-defense measures, to protect the flying public.

[29] Under this program, eligible flight crewmembers are authorized by TSA's Office of Law Enforcement/Federal Air Marshal Service to use firearms to defend against an act of criminal violence or air piracy attempting to gain control of an aircraft. A flight deck crewmember may be a pilot, flight engineer, or navigator assigned to the flight.

Figure 1: TSA Multilayered Security Approach[30]


terrorist paths
Intelligence
Customs and Border Protection
Joint Terrorism Task Force
No-Fly List and Passenger Pre-Screening
Crew Vetting
VIPR
Canines
Behavior Detection Officers
Travel Document Checker
Checkpoint/Transportation Security Officers
Checked Bags
Transportation Security Inspectors
Random Employee Screening
Bomb Appraisal Officers
Federal Air Marshal Service
Federal Flight Deck Officers
Trained Flight Crew
Law Enforcement Officers
Hardened Cockpit Door
Passengers
Layers of U.S. Aviation Security

Source: TSA.

[30] Visible Intermodal Prevention and Response (VIPR) teams augment security at key transportation

Although SOC Personnel Use Discretion When Reporting Incidents, No Formal Compliance Standards Exist

Secure Flight officials monitor aircraft operator SFPD submissions for quality and compliance, and recommend corrective action when necessary. Most compliance issues are discovered by SOC personnel during daily operations with regular monitoring of inhibited passenger BPPR and personnel reporting abnormalities. [redacted]

When aircraft operator issues occur, Watch Managers determine whether to compile a compliance package and forward it for review and investigation. Watch Managers use the Secure Flight final rule and the Consolidated User Guide as guidelines in making these determinations. The Consolidated User Guide provides technical and operational guidance and requirements to comply with the Advance Passenger Information System Pre-Departure final rule and the Secure Flight final rule, respectively.

According to Secure Flight officials, although Watch Managers have no written guidance concerning compliance issues, managers know what is expected of aircraft operators. When Watch Managers suspect a compliance issue, they collect all relevant documentation, such as call logs and Secure Flight User Interface screenshots, and forward the information via email to the Secure Flight's Industry Performance and Analysis Compliance Group. As of October 2011, the SOC was updating its notification process with automated forms.

The Industry Performance and Analysis Compliance Group analyzes the potential compliance issue and forwards the results to TSA's Offices of Security Operations or Global Strategies. These two entities then determine whether to initiate an investigation. The Industry Performance and Analysis Compliance Group

facilities in urban areas around the country. Teams work with local security and law enforcement officials to supplement existing resources, provide deterrent presence and detection capabilities, and introduce an element of unpredictably to disrupt potential terrorist planning activities.

monitors the investigations and compiles a report that provides an update on closed investigations to the SOC.

The Office of Security Operations' Compliance Programs conducts investigations for both domestic aircraft operators and foreign air carriers at domestic locations. When Compliance Programs receives a specific incident report, it conducts a preliminary investigation to determine whether to initiate a full investigation. When the investigation results in a compliance violation, Compliance Programs mails a letter of investigation requiring the aircraft operator to devise and offer a corrective action plan. Domestic aircraft operators have 20 days to respond to the letter, and foreign air carriers have 30 days to respond. The Office of Security Operations also conducts Special Emphasis Inspections to determine compliance. These are routine tests in which [redacted] the No Fly and Selectee Lists.

Compliance Programs uses a progressive enforcement method as defined in its Inspection and Enforcement Manual. Penalties usually begin with a letter of warning or administrative action, followed by fines, which are capped at $27,500. Once the compliance investigation is finished, recommendations are entered into a compliance system, which is accessed by TSA's Office of Chief Counsel. The Office of Chief Counsel gives the aircraft operators the opportunity to pay immediately, have an informal conference, or defer the action to an Administrative Law Judge.

The Office of Global Strategies deals strictly with aircraft operators overseas and foreign governments. Its authority includes international flights that depart for the United States and international flights that transit and overfly U.S. airspace. The compliance process begins when the Office of Global Strategies receives a compliance package from Secure Flight concerning a possible aircraft operator violation. The results are forwarded to the responsible Regional Operations Center within the Office of Global Strategies' Global Compliance Division, which conducts the investigation. Additionally, an International Industry Representative within the Office of Global Policy and Engagement conducts outreach to the aircraft operators and requests more information on what occurred. These results are also forwarded to the Global Compliance Division.

Office of Global Strategies officials said that the number of compliance packages has decreased as aircraft operators become more comfortable with the Secure Flight system and processes.

Although compliance issues have declined since aircraft operators cutover, Secure Flight needs defined thresholds when making compliance determinations. Without defined compliance thresholds, it is difficult to ensure that Secure Flight identifies and forwards all appropriate compliance issues.

Recommendation

We recommend that the Director of the Secure Flight program, in coordination with the Office of Security Operations Compliance Programs and Office of Global Strategies:

Recommendation #3:

Establish formal guidance that clearly defines Secure Flight program processes for reporting aircraft operator compliance issues to the Office of Security Operations and Office of Global Strategies.

Management Comments and OIG Analysis

Management Comments: TSA officials concurred with Recommendation 3. In its response, TSA said that Secure Flight has processes in place for reporting potential compliance issues to the TSA Office of Security Operations and Office of Global Strategies. In December 2011, Secure Flight organized a meeting with these offices to discuss how best to coordinate compliance issues and share information that is mutually beneficial to all three offices. TSA said that Secure Flight is currently working to schedule follow-up meetings with both offices in the near future to formalize the process.

OIG Analysis: We consider TSA's actions responsive to the intent of Recommendation 3, which is resolved and open. The recommendation will remain open pending our receipt of formalized standard operating procedures that establish clear processes for when and how to report aircraft operator compliance issues.

Secure Flight Relies on the Availability of the DHS Router, But Some Disruptions Occur

Because Secure Flight program operations are transactional, it is imperative that aircraft operators, the DHS Router, and Secure Flight maintain connectivity. Secure Flight alerts aircraft operators of upcoming routine maintenance and provides specific instructions for reporting any disruptions or connectivity issues. During disruptions, aircraft operators continue to operate by using one of six alternative options approved by Secure Flight. The frequency, duration, and monitoring of DHS Router disruptions are important to understanding potential vulnerabilities to the Federal Government's watch list matching efforts.

Secure Flight Notifies Aircraft Operators of System Maintenance

When CBP OIT conducts routine maintenance on the DHS router, CBP officials alert Secure Flight, which in turn informs aircraft operators. Secure Flight also notifies aircraft operators when it schedules maintenance to the automated matching system or to the Secure Flight test environment. These notifications provide aircraft operators with situational awareness in case any difficulties arise.

During Disruptions, TSA and CBP Work To Identify the Source

When disruptions occur, aircraft operators are typically the first to notice and initiate a reporting sequence as required in the Consolidated User Guide. Each aircraft operator has a designated point of contact who is instructed to call the SOC immediately after noticing a disruption in service, regardless of its source. Upon receiving a disruption call, a CSA documents the problem and notifies the Watch Manager. The Watch Manager initiates a service disruption procedure and conference call with TSA's Operations Support Desk to assess the situation. The Operations Support Desk opens a bridge call with CBP's OIT Technology Service Desk to start the troubleshooting process.

During the conference call, operational support staff assesses the situation to identify the problem and determine the effect of the disruption. Generally, there are [redacted] Once the disruption and effect have been identified, a severity level is established and communicated to the Watch Manager. At that time, the Watch Manager sends a disruption notification email to provide regular updates to various TSA officials and an Initial Warning Order of the service disruption to affected aircraft operators. The Watch Manager also authorizes the affected aircraft operators to use [redacted] alternate service disruption options.

Aircraft Operators Have Watch List Matching Alternatives During System Disruptions

During any type of disruption that prevents aircraft operators from receiving Secure Flight BPPR, aircraft operators have [redacted] alternatives to continue operations, described in the [redacted]

[redacted]

[redacted]

[redacted]

[redacted] which can only be accessed by authorized aircraft operator personnel.

Although these options are available to aircraft operators, several airline industry partners we spoke with said that aircraft [redacted] Some officials at DHS, TSA, and the TSC discussed [redacted] However, aircraft operators currently use the watch list to [redacted]

[redacted] Secure Flight officials explained, however, that as a result of the TSA and CBP Chief Information Officers' efforts to prioritize the resolution [redacted] the relationship between the two components has improved. Both components worked together to develop a formal procedure to isolate and resolve disruptions, and keep all parties informed of disruption status. Additionally, CBP OIT and Secure Flight have weekly management and technical meetings, and both appear satisfied with continuing communication improvements.

Monitoring the DHS Router Consistently Appears Problematic

[redacted]

[redacted]

The data provided by Secure Flight and CBP OIT indicate [redacted] For example, between January 1 and July 31, 2011, CBP OIT reported—

- [redacted]

Secure Flight, however, reported [redacted]

[redacted] Due to the essential nature of information received and transmitted by the DHS Router, our office may review these issues at a later date.

<u>Secure Flight Has Full Site Redundancy and Conducts System Testing To Ensure Availability</u>

To reduce possible disruptions and ensure availability, TTAC Technology conducts Secure Flight system and regression testing and monitors the system continuously. Secure Flight program officials also conduct routine tests on aircraft operators to confirm receipt of SFPD when system changes occur. Secure Flight has redundant systems and sites, which allow passenger information matching to continue should one site or system experience a disruption.

TTAC Technology Conducts System Testing

Before new releases or updates to the Secure Flight system are implemented, TTAC Technology conducts performance and regression testing in a simulated environment to ensure appropriate functionality. TTAC Technology applies a new system release to the test environment system to determine whether the release causes any errors or unnecessarily slows the system. TTAC Technology conducts these tests again once the release has been fully implemented to the automated matching system to verify that there are no adverse system effects that were not present in the test environment. These tests also check the system's capacity to manage high-volume periods and high-priority response times. TTAC Technology monitors the system, including automatic linkages, interfaces, and network connectivity to the DHS Router, and alerts relevant parties when there are issues with aircraft operator connections.

Although TTAC Technology is responsible for ensuring system availability, Secure Flight's Industry Performance and Analysis office conducts routine Production Validation Testing of aircraft operator SFPD submissions. This replicates some of the testing Industry Performance and Analysis uses to test aircraft operators during cutover. Replication, however, validates that, despite changes to Secure Flight's system and possible changes to the aircraft operator systems, Secure Flight is receiving data properly and receiving complete SFPD during transmissions.

Secure Flight Has Site and System Redundancy

In addition to TTAC Technology and Secure Flight program testing, Secure Flight operations were designed to be redundant, and to reduce the likelihood and duration of outages. This includes two fully redundant SOC sites and systems in geographically dispersed locations: Annapolis Junction, MD, and Colorado Springs, CO. Both operation centers have full-time personnel and servers that run simultaneously every day. Each site can handle full operations should the other site experience difficulties. This redundancy helps to ensure that at least one server is running continuously. If there is a disruption, either location handles all resolution calls and SFPD information vetting.

In addition, Secure Flight has a continuity of operations plan and a continuity manager. During our fieldwork, continuity training was being developed and the continuity of operations plan was being expanded. The redundancy of Secure Flight's systems and sites was tested on August 23, 2011, when a 5.8 magnitude earthquake affected Government operations throughout the east coast. As the Maryland center was evacuated, continuity officers alerted the Colorado center regarding the disruption. SOC and program officials confirmed that the automatic switching or failover to the Colorado site was executed according to the continuity of operations plan. The failover did not stress operations. During this time, additional analysts were placed on standby at the Colorado site in case building inspectors were unable to clear the Maryland site for operations within 24 hours. The Maryland site remained closed from approximately 2:00 p.m. to 11:30 p.m., and Secure Flight officials said that no disruption to passenger screening occurred.

Secure Flight Has Developed Safeguards To Protect Personal Data and Watch List Records

Secure Flight has developed procedures to ensure that passengers are aware of information requirements and how to obtain additional information regarding the collection and use of this data. Secure Flight has a privacy program that adheres to Government standards and ensures that personnel are adequately trained.

Secure Flight Receives Minimal Personal Data and Limits External Requests

Secure Flight receives the minimal passenger personal data required to conduct effective passenger matching against the No Fly List, Selectee List, and other lists. TSA also requires aircraft operators to provide a specified privacy notice on their websites or self-service kiosks prior to collecting passenger or nontraveler information. This privacy notice informs passengers of the data required to enter the boarding area and that this information may be shared with law enforcement, intelligence agencies, or others under its System of Records Notice. It refers passengers to the published System of Records Notice and Privacy Impact Assessment. The System of Records Notice specifies the circumstances under which Secure Flight records or information may be shared, for what purposes, and with whom. The Privacy Impact Assessment is used to identify and mitigate privacy risks of collecting, maintaining, and disseminating Secure Flight information. Aircraft operators must also ensure that third-party reservation websites provide this privacy notice prior to collecting passenger information.

According to DHS officials, Secure Flight also limits personal data and information requests from external agencies and limits requests to those related to terrorism and national transportation security. When an external request is received, it must be reviewed by the TSA Office of Chief Counsel and TSA Office of Privacy. The Privacy Impact Assessment helps the public understand what personal data are being collected, why they are being collected, and how they will be used. TSA's Privacy Office recently formalized the annual review of the Privacy Impact Assessment, which includes determining whether the program is still operating in accordance with the published Privacy Impact Assessment or whether the assessment requires updating. In August 2011, Secure Flight updated its Privacy Impact Assessment to address new initiatives, such as Known Traveler. The Known Traveler initiative aims to identify low-risk passengers and expedite their screening process.

Secure Flight Has a Privacy Program To Protect Passenger Data and Provides Additional Privacy Training To Secure Flight Personnel

In addition to these public notices, Secure Flight has developed and implemented a comprehensive privacy program to protect SFPD personally identifiable information provided by aircraft operators. According to the Secure Flight Concept of Operations, the privacy program meets all privacy standards set forth by the U.S. Government, aligns with TSA privacy principles, complies with industry best practices, and provides a defined redress process. The TSA Privacy Office has a Privacy Officer colocated with Secure Flight to ensure that privacy is addressed in all aspects of the program, from developing initiatives to releasing system updates.

Secure Flight ensures that employees receive privacy training required of all TSA employees as well as additional and recurrent Secure Flight privacy training. To manage personally identifiable information and sensitive watch list data, Secure Flight restricts physical access to the SOC and has user-controlled system access, which is based on what each person needs to know to perform his or her duties. Documents containing personal data or sensitive information are password protected when sent via email. To prevent the disclosure of personal data to unauthorized users, Secure Flight has an authentication process for eSecure Flight users and for aircraft operators placing resolution calls. The Secure Flight Privacy Officer conducts privacy compliance audits and an ad hoc review of passenger information entered into the Secure Flight User Interface. Any issues are reported to TSA's Privacy Office.

Secure Flight also follows privacy standards for retaining personally identifiable information and regularly purges privacy data. For example, as approved by the National Archives and Records Administration, the Secure Flight records retention schedule provides for a retention period of 7 days for individuals who are not a match to the Government watch list, 7 years for individuals who are a potential match, and 99 years for individuals who are a confirmed match. The Secure Flight Privacy Officer also conducts weekly purge compliance spot checks.

Secure Flight Should Prioritize Its Mission, While Developing and Implementing Initiatives

Although Secure Flight has been screening domestic and international commercial aircraft operator passengers for around 1 year, the program has taken on or participated in developing a series of new initiatives: WLS, overflights, risk-based security, barcode encryption on boarding passes, and a Joint Analysis Center. DHS Offices of Privacy and for Civil Rights and Civil Liberties are consulted during initiative development, as appropriate. While these initiatives may help to improve the efficiency and effectiveness of passenger prescreening, it is prudent for Secure Flight to prioritize and focus on its mission and mandate.

Watch List Service Changes Will Enhance Secure Flight Processes, But Delays Exist

During our fieldwork, Secure Flight was receiving daily updates from the TSDB, with urgent updates as necessary. Secure Flight began implementing a change, which will serve as an improved method of transmitting data from the TSC to Secure Flight. Secure Flight will now connect to CBP to access the WLS, a near real-time export of the TSDB, which will eliminate the need for a daily export to the SOC. When the TSC adds, modifies, or deletes data from the TSDB, the WLS export of the TSDB will be automatically synchronized. This change is expected to result in a more timely and accurate match review process, which is essential to Secure Flight's operational effectiveness. Although the final WLS rollout was expected by spring 2011, Secure Flight delayed implementation to complete testing the Known Traveler program. At the end of our fieldwork, DHS officials estimated that the WLS changeover would be implemented in the first quarter of 2012.

Secure Flight Has Developed Guidelines for Overflight Implementation

The Secure Flight final rule covers aircraft operators overflying the continental United States, excluding some domestic flights within Canada and Mexico that transit U.S. airspace. A flight not required to submit SFPD, for example, would include a flight from Montreal, Canada, to Halifax, Canada, although a portion of this flight transits U.S. airspace. During overflight requirements development, implementation was deferred, but a pilot test occurred on May 26, 2011, with an Air France flight from Paris, France, to Mexico City, Mexico. The draft overflight requirements were submitted to foreign air carriers for review and comment, and the Office of Global Strategies and Secure Flight received responses from August 15 to September 30, 2011. Subsequent to the completion of our fieldwork, TSA officials notified us that the comments have been reviewed and addressed, and the requirements approved by the TSA Administrator. The final Model Security Program was published on February 8, 2012, and foreign air carriers had until March 8, 2012, to comply.

To prevent confusion on what flights are considered overflights, Secure Flight officials obtained data from the FAA concerning flight routes that transit continental U.S. airspace or come within 12 nautical miles of the U.S. coastline. From this information, Secure Flight developed a list of airport pairs or combinations of departure and arrival airports. Flights between these airports will be considered overflights, requiring aircraft operators to submit SFPD information. A Secure Flight official said that airport pairs will need to be reviewed on a continuous basis as new flight patterns are added. In addition, Secure Flight officials estimate that the airport pair configuration would add approximately 78,000 flights per year and 20,000 passengers per day. As the Secure Flight program currently vets more than 2 million passengers per day, the additional overflight passengers are not expected to stress the system or analysts' ability to perform SFPD information prescreening against the watch list.

Implementation of overflight screening will also include procedural differences. For example, Secure Flight will neither inhibit nor provide foreign aircraft operators with notifications of passenger matches to the Do Not Board List. Further, Secure Flight can only recommend additional screening for passenger matches to the Selectee List, and foreign aircraft operators may board No Fly List passenger matches, but these flights must be diverted from U.S. airspace. During our fieldwork, Secure Flight was developing a standard operating procedure for reporting these instances to the FAA and TSA.

Secure Flight Is Integrating a Risk-Based Security Approach

TSA has also started developing a multi-phased risk-based security initiative in which Secure Flight will be a key facilitator of these initiatives. The concept of risk-based security is to develop and designate an appropriate screening level based on varying passenger risks. The first phase of the risk-based security initiative is the Known Traveler pilot, publicly referred to as Pre✓™. While Known Traveler helps identify low-risk passengers, TSA OI and Secure Flight are beginning to develop a second phase of risk-based security, which will identify a new category of high-risk passengers to receive additional screening.

Known Traveler passengers could be allowed to process through airport security without removing their shoes or laptop computers from their carry bags. Secure Flight combined elements of CBP's Global Entry program and worked with Delta Airlines and American Airlines to identify low-risk passengers participating in frequent flier programs, as well as participants in similar CBP programs for low-risk travelers to receive expedited border screening.[32]

As Known Traveler passengers are vetted, those meeting established criteria receive a designation in their SFPD. When Known Traveler passengers fly, their SFPD is still vetted through the Secure Flight system for watch list matching. When cleared through the automated matching system, their trusted traveler status is encoded into a barcode, which is decoded with special boarding pass scanners that Transportation Security Officers use at security checkpoints. Private industry partners have voiced support for the Known Traveler pilot, which screened 40,000 passengers in October 2011 and is expanding.

TSA Is Developing Special Boarding Pass Scanners To Address Vulnerabilities

Federal Government and private industry partners raised concerns that passengers can submit false data and present false credentials or identity documents to gain access to aircraft or sterile areas. To address this concern, TSA and Secure Flight are developing technology to use boarding pass scanners to help authenticate identity documents to ensure that all SFPD information matches the information on an individual's identity document. This effort is called the Credential Authentication Technology – Boarding Pass Scanning Systems Initiative.

Some of this technology is currently being used as part of the Pre✓™ pilot. For the Credential Authentication Technology – Boarding Pass Scanning Systems Initiative, TSA and Secure Flight are working to add an encrypted data block, which would include a passenger's name, date of birth, gender, screening status, itinerary, and a date stamp. Secure Flight plans to send an encrypted code to the aircraft operator to insert, but not interpret, on the boarding pass. Transportation Security Officers will use boarding pass scanners to verify the authenticity of the identification, while also verifying that the identification information matches

[32] Global Entry, intended for frequent international travelers, allows expedited clearance for preapproved, low-risk travelers upon arrival in the United States. Program participants proceed to Global Entry kiosks at airports, present their machine-readable passport or U.S. permanent resident card, place their fingertips on the scanner for fingerprint verification, and make a customs declaration. All applicants undergo a rigorous background check and interview before enrollment.

passenger-submitted SFPD. Existing boarding pass scanners from Pre✓™ will need to be modified to decrypt the data block at the checkpoints. Secure Flight estimates that this capability will be ready to pilot by April 2012.

Communication Difficulties Exist in the Development and Implementation of New Initiatives

Although Federal Government and private industry partners have acknowledged that the Known Traveler pilot results are successful, collaboration and communication difficulties have persisted throughout this and other Secure Flight initiatives.

Private industry officials note that communication between TSA and aircraft operators could be clearer and timelier during the planning stages. Confusion among Secure Flight, TTAC, and private industry officials persists because of the inconsistent program naming. For example, the Pre✓™ program was referred to as Known Traveler and Trusted Traveler before it was publicly renamed Pre✓™ just days before the pilot started. Although this program leverages elements and screening eligibility determinations from several CBP programs, the DHS Screening Coordination Office was not involved in planning or coordinating the program's rollout.

Although Secure Flight has received data from the FAA, it has not worked with the FAA to develop the list of airport pairs used to determine overflights. As Secure Flight must rely on the FAA to help monitor overflight diversions, as well as to continue reviewing airport pair determinations as new routes are added, developing a working relationship would be beneficial to both entities. In its written response to the draft report, TSA said that Secure Flight and the FAA have had an established working relationship for overflights requirements since 2007. However, interviews with FAA officials during our review indicate that the FAA did not perceive the relationship as collaborative. The FAA was also afforded an opportunity to review and clarify language in the draft report, and did not suggest any changes.

Secure Flight is also piloting and implementing a general aviation prescreening initiative. This initiative has been called General Aviation and the Twelve-Five program interchangeably by Secure Flight officials. A Secure Flight official identified these aircraft as "unscheduled and/or private charters weighing 12,500 pounds." However, the updated Secure Flight Privacy Impact Assessment allows operators and lessors of "Twelve-Five aircraft" to use Secure Flight. These operators and lessors are described as "charter operators and lessors of aircraft with a maximum takeoff weight in excess of 12,500 pounds, and scheduled aircraft operators under 49 CFR 1544.101(d)."[33] Furthermore, FAA officials confirmed that pilots understand general aviation to specifically refer to unscheduled, non-hirable flights. FAA officials also said that referring interchangeably to the initiative as the General Aviation and Twelve-Five program would be confusing to aircraft operators, who understand this terminology to mean something different.

Recommendation

We recommend that the Administrator of the Transportation Security Administration, in coordination with the Secure Flight program:

Recommendation #4:

Develop a communication strategy to formalize coordination and collaboration with Federal Government and private industry partners to ensure clarity when developing and implementing new initiatives.

Management Comments and OIG Analysis

Management Comments: TSA officials did not concur with Recommendation 4. In its response, TSA said that it has already developed and implemented a comprehensive communication strategy to formalize coordination and collaboration with Federal Government and private industry partners to ensure clarity when developing and implementing new initiatives. Additionally, Secure Flight already develops and maintains stakeholder assessments for its specific initiatives, hosts semi-annual aviation industry conferences, and disseminates informational Secure Flight Updates to aircraft operators to ensure that

[33] Privacy Impact Assessment Update for Secure Flight, August 15, 2011, p. 2.

consistent and reliable messaging is provided to Secure Flight stakeholders. Therefore, with respect to Secure Flight, TSA considers action for this recommendation complete.

TSA noted that this recommendation is based on findings cited in the report regarding initiatives (i.e., Known Traveler, TSA Pre✓™) that are TSA-wide initiatives under Risk-Based Security. Each of the pilot programs has a tailored communications strategy that evolves depending upon the results of the pilot program and decisions on system-wide implementation.

OIG Analysis: Although TSA did not concur with this recommendation, we consider the actions responsive to the intent of Recommendation 4, which is resolved and open. The recommendation will remain open pending our receipt of TSA's communication strategy with Federal Government partners and private industry partners. To address the intent of this recommendation, the communication strategy should include communication activities that foster a collaborative working relationship with Federal Government and private industry partners. The strategy should also outline general roles and responsibilities for Secure Flight when the program communicates directly with Federal Government and private industry partners about new initiatives.

The Joint Analysis Center Further Examines Secure Flight Data To Identify Trends and Patterns

In addition to Secure Flight's efforts to improve the efficiency and effectiveness of passenger prescreening, TSA, in conjunction with Secure Flight, has developed the Joint Analysis Center. This center is colocated within the SOC and uses encounter match data to perform broader aviation security analysis. Analysts located at Secure Flight work jointly with TTAC and TSA OI analysts to use passenger vetting results from Secure Flight and other programs to identify trends and patterns in aviation security.

For example, trends and patterns might include which aircraft operators or specific flights have the most Selectee List matches, or whether an individual on the Selectee List departs from a particular airport or consistently travels with other individuals who are a match to the watch list. This information is shared with other Federal Government partners and may be used to inform tactical decisions. As an example, when the Joint Analysis Center determines that a large number of Selectees routinely fly into or out of a particular airport, it will present the data to TSA leadership to drive operational decisions.

Conclusion

Public and private partners recognize the Secure Flight program's value, as it has provided more consistent passenger prescreening. [redacted] it has a defined system and processes to conduct watch list matching. To ensure that aircraft operators follow established procedures, the SOC monitors records and forwards issues for compliance investigation. However, this process is not standardized, and program officials send compliance packages using their discretion. Once Secure Flight successfully cutover aircraft operators, the program focus shifted toward addressing emerging threats through multiple initiatives. To develop and implement these initiatives effectively, Secure Flight must enhance its relationship and communication efforts with public and private partners.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

We reviewed the implementation and coordination of TSA's Secure Flight program. Our objectives were to determine (1) whether the program is screening all appropriate persons; (2) whether processes and standards for aircraft operators to submit SFPD information and receive BPPR instructions are timely and effective; (3) how the program's screening processes are tested for accuracy, prioritization, and timeliness during high-volume periods; and (4) how Secure Flight is protecting varying layers of personally identifiable and sensitive watch list information.

We reviewed the communication processes and capabilities between the Secure Flight program and aircraft operators and other relevant Government partners. We examined directives, policies, and procedures relating to these processes and their intended purpose. In addition, we reviewed relevant memorandums of agreement and understanding between TSA and its Government partners with a role in prescreening international and domestic passengers against the Federal Government's terrorist watch list.

We interviewed TSA officials from the following offices: Secure Flight program and operations, TTAC, OI, DHS TRIP, Office of Privacy, Transportation Sector Network Management, Office of Global Strategies, and Office of Security Operations. In addition, we met with officials from the DHS Office for Civil Rights and Civil Liberties, CBP, DHS Screening Coordination Office, the FAA, and the FBI. Further, we engaged airline industry associations and aircraft operators. This allowed us to assess the effectiveness of Secure Flight's efforts, as well as the level of communication and collaboration between Secure Flight and its Federal Government and private sector partners in the passenger prescreening process.

We also reviewed applicable legislation, regulations, directives, policies, operating procedures, and official guidance documents and manuals. In addition, we studied work previously performed by our office in this and associated areas, as well as the work conducted by the Government Accountability Office.

We conducted this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
Recommendations

We recommend that the Director of the Secure Flight program:

Recommendation #1:

Identify how and when aircraft operators override an inhibited boarding pass printing result and implement corrective action to eliminate unauthorized overrides by aircraft operators.

Recommendation #2:

Ensure that aircraft operators prioritize Secure Flight passenger data appropriately and receive an accurate, updated boarding pass printing result when aircraft operators submit changes.

We recommend that the Director of the Secure Flight program, in coordination with the Office of Security Operations Compliance Programs and Office of Global Strategies:

Recommendation #3:

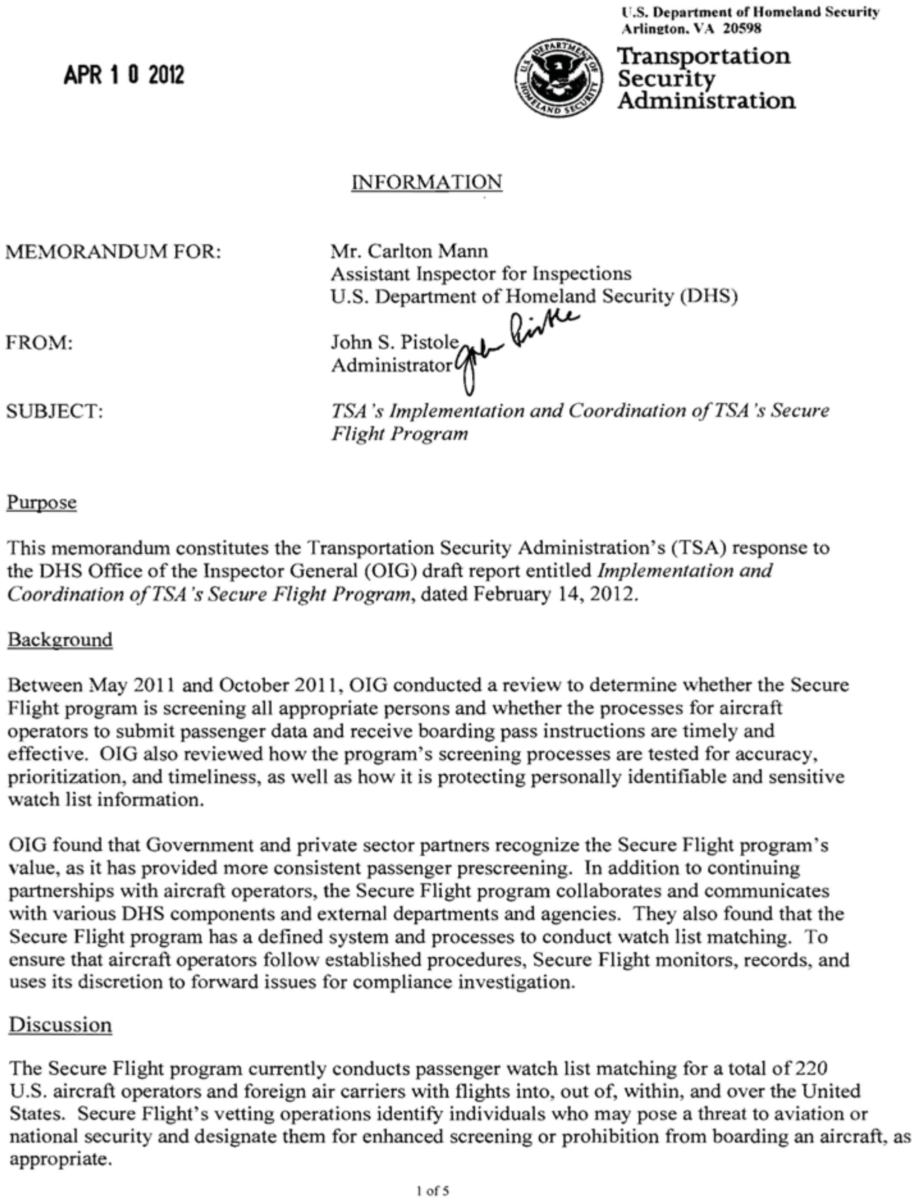
Establish formal guidance that clearly defines Secure Flight program processes for reporting aircraft operator compliance issues to the Office of Security Operations and Office of Global Strategies.

We recommend that the Administrator of the Transportation Security Administration, in coordination with the Secure Flight program:

Recommendation #4:

Develop a communication strategy to formalize coordination and collaboration with Federal Government and private industry partners to ensure clarity when developing and implementing new initiatives.

Appendix C
Management Comments to the Draft Report



U.S. Department of Homeland Security
Arlington, VA 20598

Transportation
Security
Administration

APR 1 0 2012

INFORMATION

MEMORANDUM FOR: Mr. Carlton Mann
Assistant Inspector for Inspections
U.S. Department of Homeland Security (DHS)

FROM: John S. Pistole
Administrator

SUBJECT: *TSA's Implementation and Coordination of TSA's Secure Flight Program*

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to the DHS Office of the Inspector General (OIG) draft report entitled *Implementation and Coordination of TSA's Secure Flight Program*, dated February 14, 2012.

Background

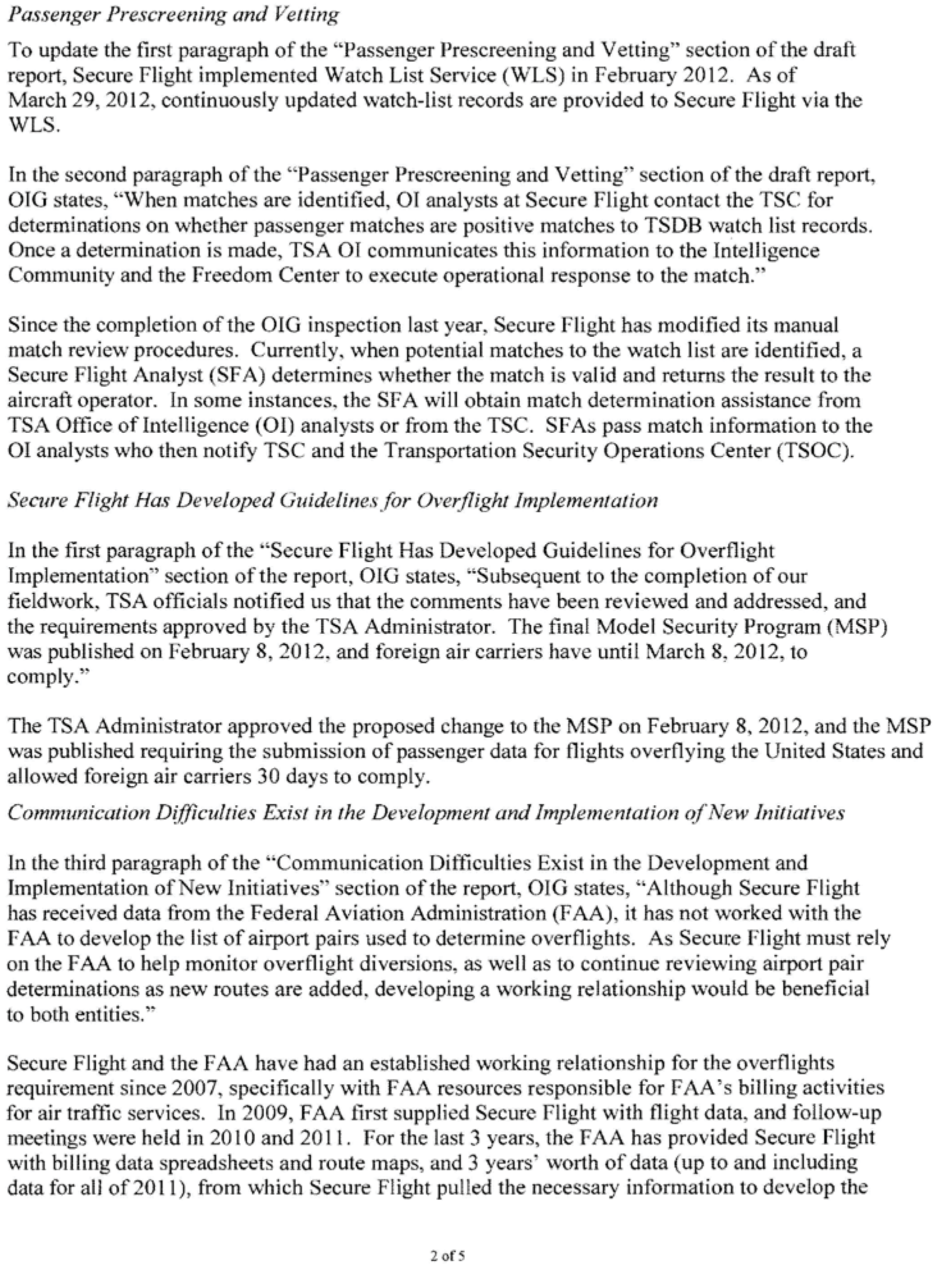
Between May 2011 and October 2011, OIG conducted a review to determine whether the Secure Flight program is screening all appropriate persons and whether the processes for aircraft operators to submit passenger data and receive boarding pass instructions are timely and effective. OIG also reviewed how the program's screening processes are tested for accuracy, prioritization, and timeliness, as well as how it is protecting personally identifiable and sensitive watch list information.

OIG found that Government and private sector partners recognize the Secure Flight program's value, as it has provided more consistent passenger prescreening. In addition to continuing partnerships with aircraft operators, the Secure Flight program collaborates and communicates with various DHS components and external departments and agencies. They also found that the Secure Flight program has a defined system and processes to conduct watch list matching. To ensure that aircraft operators follow established procedures, Secure Flight monitors, records, and uses its discretion to forward issues for compliance investigation.

Discussion

The Secure Flight program currently conducts passenger watch list matching for a total of 220 U.S. aircraft operators and foreign air carriers with flights into, out of, within, and over the United States. Secure Flight's vetting operations identify individuals who may pose a threat to aviation or national security and designate them for enhanced screening or prohibition from boarding an aircraft, as appropriate.

1 of 5



Passenger Prescreening and Vetting

To update the first paragraph of the "Passenger Prescreening and Vetting" section of the draft report, Secure Flight implemented Watch List Service (WLS) in February 2012. As of March 29, 2012, continuously updated watch-list records are provided to Secure Flight via the WLS.

In the second paragraph of the "Passenger Prescreening and Vetting" section of the draft report, OIG states, "When matches are identified, OI analysts at Secure Flight contact the TSC for determinations on whether passenger matches are positive matches to TSDB watch list records. Once a determination is made, TSA OI communicates this information to the Intelligence Community and the Freedom Center to execute operational response to the match."

Since the completion of the OIG inspection last year, Secure Flight has modified its manual match review procedures. Currently, when potential matches to the watch list are identified, a Secure Flight Analyst (SFA) determines whether the match is valid and returns the result to the aircraft operator. In some instances, the SFA will obtain match determination assistance from TSA Office of Intelligence (OI) analysts or from the TSC. SFAs pass match information to the OI analysts who then notify TSC and the Transportation Security Operations Center (TSOC).

Secure Flight Has Developed Guidelines for Overflight Implementation

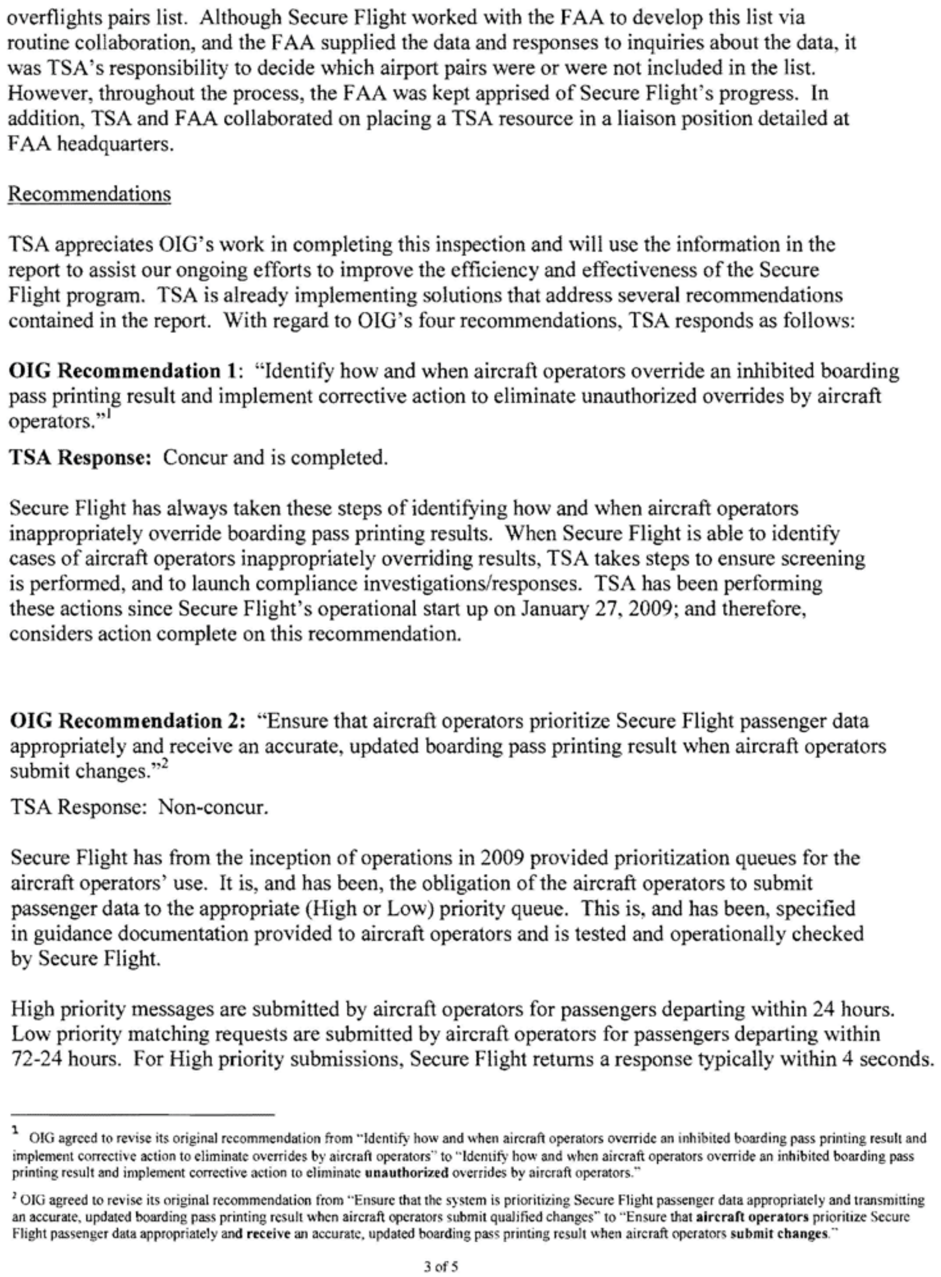
In the first paragraph of the "Secure Flight Has Developed Guidelines for Overflight Implementation" section of the report, OIG states, "Subsequent to the completion of our fieldwork, TSA officials notified us that the comments have been reviewed and addressed, and the requirements approved by the TSA Administrator. The final Model Security Program (MSP) was published on February 8, 2012, and foreign air carriers have until March 8, 2012, to comply."

The TSA Administrator approved the proposed change to the MSP on February 8, 2012, and the MSP was published requiring the submission of passenger data for flights overflying the United States and allowed foreign air carriers 30 days to comply.

Communication Difficulties Exist in the Development and Implementation of New Initiatives

In the third paragraph of the "Communication Difficulties Exist in the Development and Implementation of New Initiatives" section of the report, OIG states, "Although Secure Flight has received data from the Federal Aviation Administration (FAA), it has not worked with the FAA to develop the list of airport pairs used to determine overflights. As Secure Flight must rely on the FAA to help monitor overflight diversions, as well as to continue reviewing airport pair determinations as new routes are added, developing a working relationship would be beneficial to both entities."

Secure Flight and the FAA have had an established working relationship for the overflights requirement since 2007, specifically with FAA resources responsible for FAA's billing activities for air traffic services. In 2009, FAA first supplied Secure Flight with flight data, and follow-up meetings were held in 2010 and 2011. For the last 3 years, the FAA has provided Secure Flight with billing data spreadsheets and route maps, and 3 years' worth of data (up to and including data for all of 2011), from which Secure Flight pulled the necessary information to develop the



overflights pairs list. Although Secure Flight worked with the FAA to develop this list via routine collaboration, and the FAA supplied the data and responses to inquiries about the data, it was TSA's responsibility to decide which airport pairs were or were not included in the list. However, throughout the process, the FAA was kept apprised of Secure Flight's progress. In addition, TSA and FAA collaborated on placing a TSA resource in a liaison position detailed at FAA headquarters.

Recommendations

TSA appreciates OIG's work in completing this inspection and will use the information in the report to assist our ongoing efforts to improve the efficiency and effectiveness of the Secure Flight program. TSA is already implementing solutions that address several recommendations contained in the report. With regard to OIG's four recommendations, TSA responds as follows:

OIG Recommendation 1: "Identify how and when aircraft operators override an inhibited boarding pass printing result and implement corrective action to eliminate unauthorized overrides by aircraft operators."[1]

TSA Response: Concur and is completed.

Secure Flight has always taken these steps of identifying how and when aircraft operators inappropriately override boarding pass printing results. When Secure Flight is able to identify cases of aircraft operators inappropriately overriding results, TSA takes steps to ensure screening is performed, and to launch compliance investigations/responses. TSA has been performing these actions since Secure Flight's operational start up on January 27, 2009; and therefore, considers action complete on this recommendation.

OIG Recommendation 2: "Ensure that aircraft operators prioritize Secure Flight passenger data appropriately and receive an accurate, updated boarding pass printing result when aircraft operators submit changes."[2]

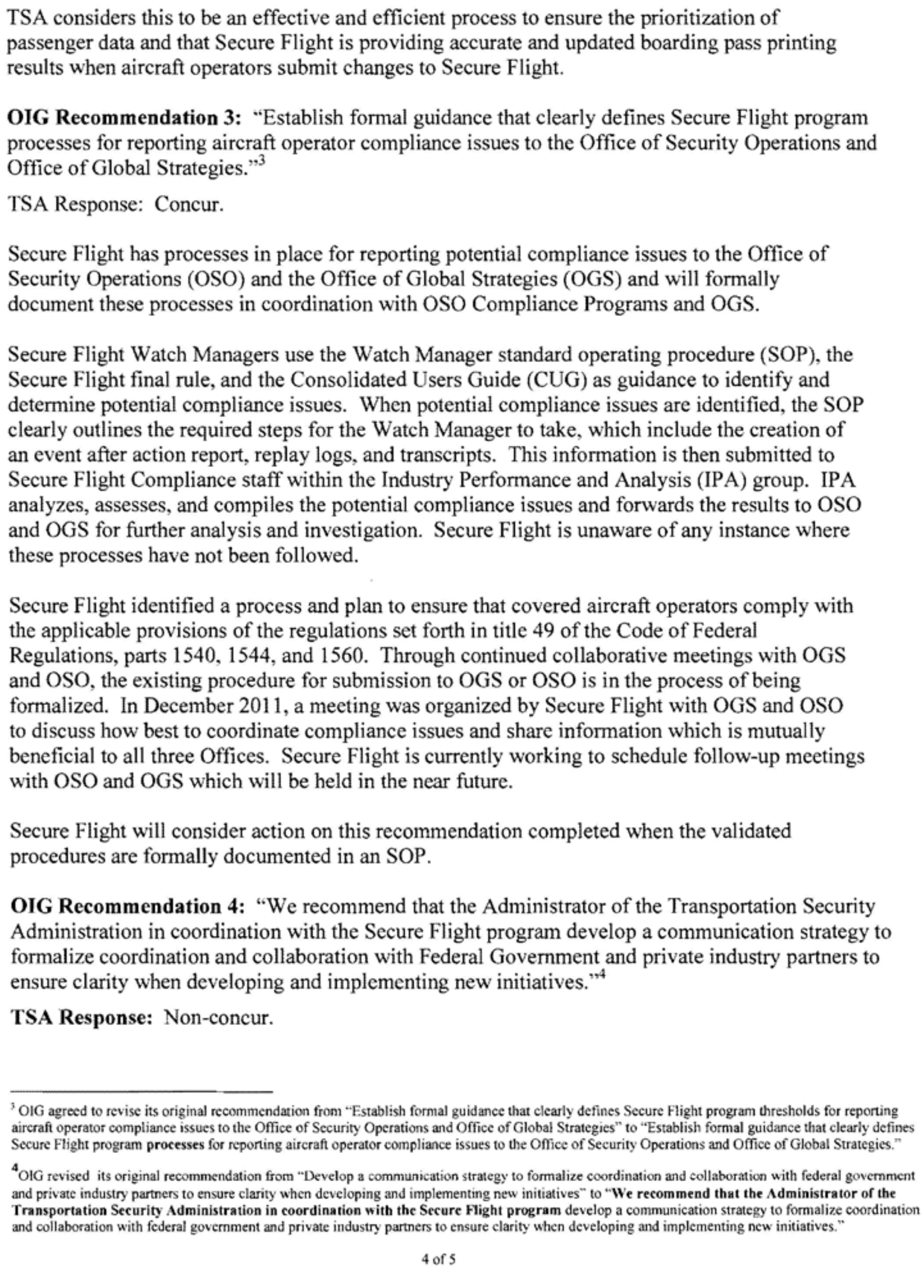
TSA Response: Non-concur.

Secure Flight has from the inception of operations in 2009 provided prioritization queues for the aircraft operators' use. It is, and has been, the obligation of the aircraft operators to submit passenger data to the appropriate (High or Low) priority queue. This is, and has been, specified in guidance documentation provided to aircraft operators and is tested and operationally checked by Secure Flight.

High priority messages are submitted by aircraft operators for passengers departing within 24 hours. Low priority matching requests are submitted by aircraft operators for passengers departing within 72-24 hours. For High priority submissions, Secure Flight returns a response typically within 4 seconds.

[1] OIG agreed to revise its original recommendation from "Identify how and when aircraft operators override an inhibited boarding pass printing result and implement corrective action to eliminate overrides by aircraft operators" to "Identify how and when aircraft operators override an inhibited boarding pass printing result and implement corrective action to eliminate **unauthorized** overrides by aircraft operators."

[2] OIG agreed to revise its original recommendation from "Ensure that the system is prioritizing Secure Flight passenger data appropriately and transmitting an accurate, updated boarding pass printing result when aircraft operators submit qualified changes" to "Ensure that **aircraft operators** prioritize Secure Flight passenger data appropriately and **receive** an accurate, updated boarding pass printing result when aircraft operators **submit changes**."



TSA considers this to be an effective and efficient process to ensure the prioritization of passenger data and that Secure Flight is providing accurate and updated boarding pass printing results when aircraft operators submit changes to Secure Flight.

OIG Recommendation 3: "Establish formal guidance that clearly defines Secure Flight program processes for reporting aircraft operator compliance issues to the Office of Security Operations and Office of Global Strategies."[3]

TSA Response: Concur.

Secure Flight has processes in place for reporting potential compliance issues to the Office of Security Operations (OSO) and the Office of Global Strategies (OGS) and will formally document these processes in coordination with OSO Compliance Programs and OGS.

Secure Flight Watch Managers use the Watch Manager standard operating procedure (SOP), the Secure Flight final rule, and the Consolidated Users Guide (CUG) as guidance to identify and determine potential compliance issues. When potential compliance issues are identified, the SOP clearly outlines the required steps for the Watch Manager to take, which include the creation of an event after action report, replay logs, and transcripts. This information is then submitted to Secure Flight Compliance staff within the Industry Performance and Analysis (IPA) group. IPA analyzes, assesses, and compiles the potential compliance issues and forwards the results to OSO and OGS for further analysis and investigation. Secure Flight is unaware of any instance where these processes have not been followed.

Secure Flight identified a process and plan to ensure that covered aircraft operators comply with the applicable provisions of the regulations set forth in title 49 of the Code of Federal Regulations, parts 1540, 1544, and 1560. Through continued collaborative meetings with OGS and OSO, the existing procedure for submission to OGS or OSO is in the process of being formalized. In December 2011, a meeting was organized by Secure Flight with OGS and OSO to discuss how best to coordinate compliance issues and share information which is mutually beneficial to all three Offices. Secure Flight is currently working to schedule follow-up meetings with OSO and OGS which will be held in the near future.

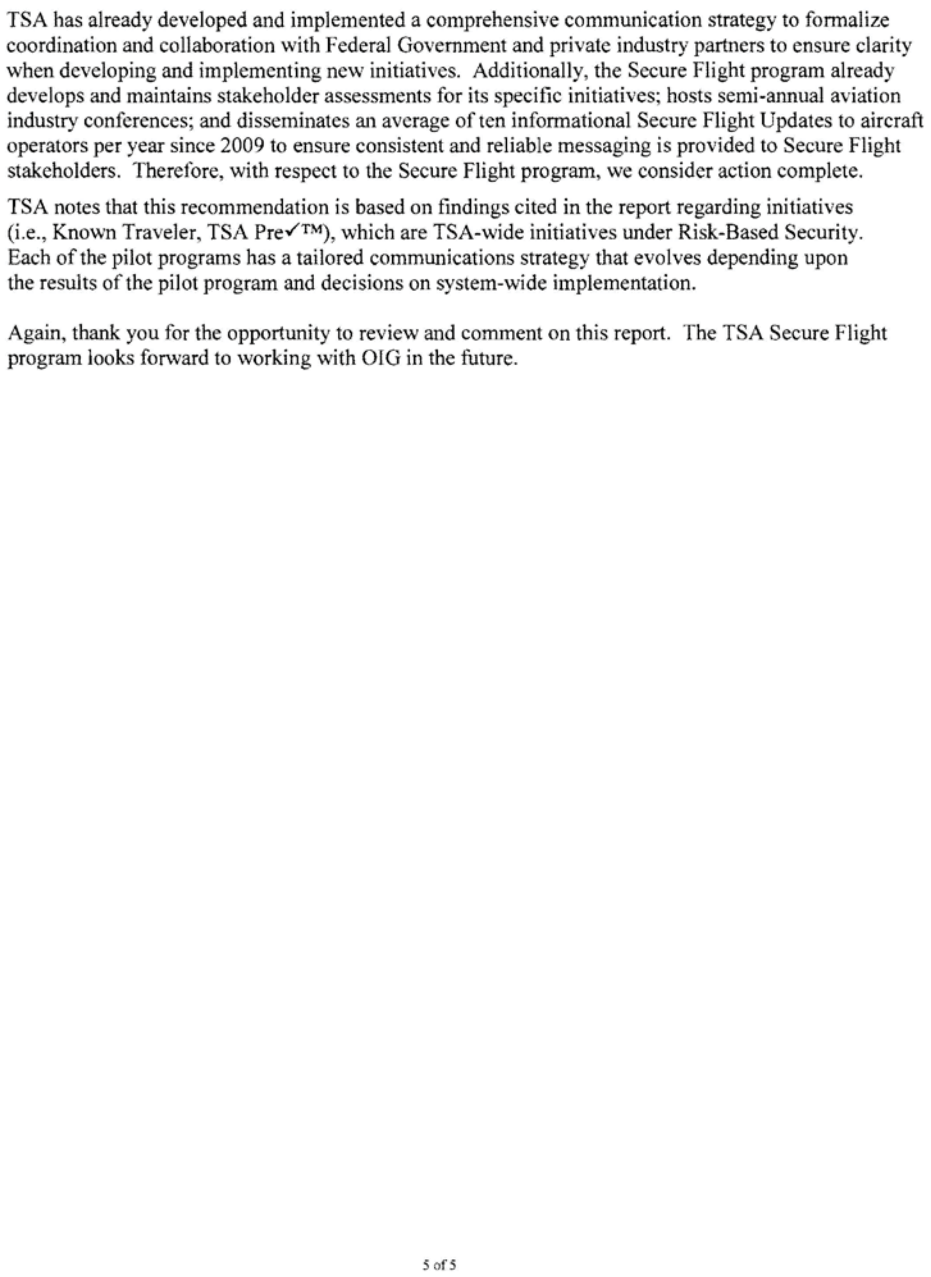
Secure Flight will consider action on this recommendation completed when the validated procedures are formally documented in an SOP.

OIG Recommendation 4: "We recommend that the Administrator of the Transportation Security Administration in coordination with the Secure Flight program develop a communication strategy to formalize coordination and collaboration with Federal Government and private industry partners to ensure clarity when developing and implementing new initiatives."[4]

TSA Response: Non-concur.

[3] OIG agreed to revise its original recommendation from "Establish formal guidance that clearly defines Secure Flight program thresholds for reporting aircraft operator compliance issues to the Office of Security Operations and Office of Global Strategies" to "Establish formal guidance that clearly defines Secure Flight program **processes** for reporting aircraft operator compliance issues to the Office of Security Operations and Office of Global Strategies."

[4] OIG revised its original recommendation from "Develop a communication strategy to formalize coordination and collaboration with federal government and private industry partners to ensure clarity when developing and implementing new initiatives" to "**We recommend that the Administrator of the Transportation Security Administration in coordination with the Secure Flight program** develop a communication strategy to formalize coordination and collaboration with federal government and private industry partners to ensure clarity when developing and implementing new initiatives."

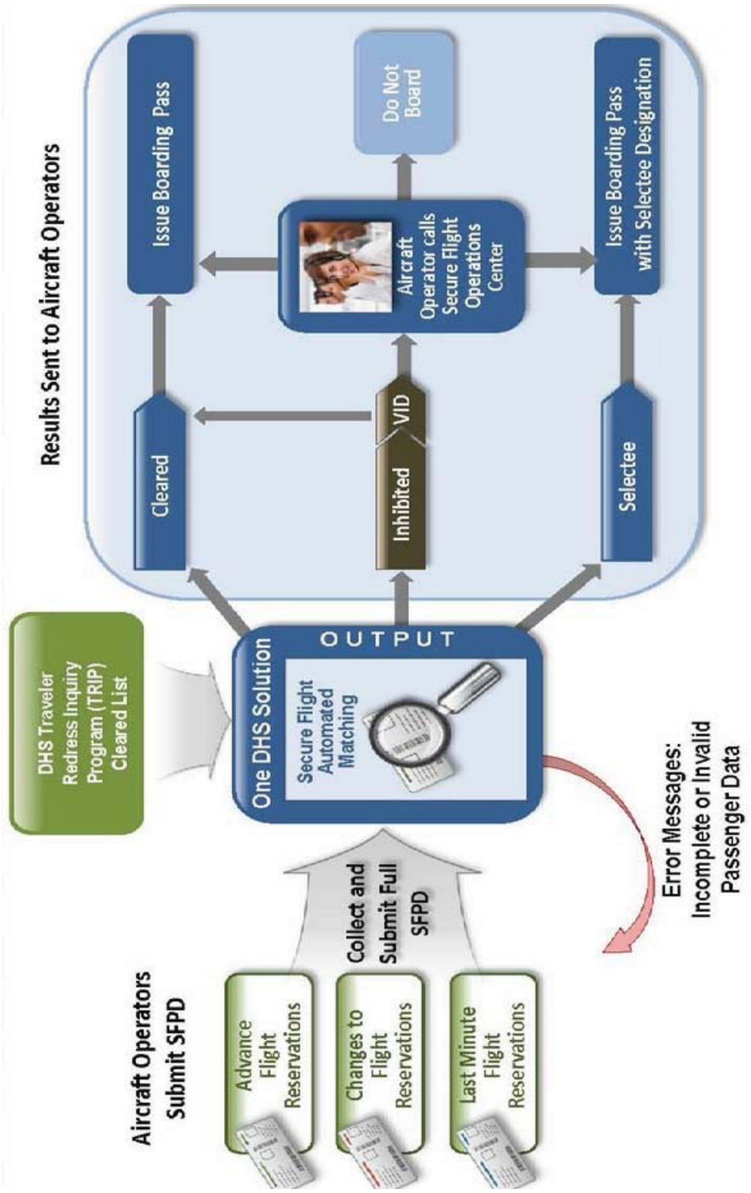


TSA has already developed and implemented a comprehensive communication strategy to formalize coordination and collaboration with Federal Government and private industry partners to ensure clarity when developing and implementing new initiatives. Additionally, the Secure Flight program already develops and maintains stakeholder assessments for its specific initiatives; hosts semi-annual aviation industry conferences; and disseminates an average of ten informational Secure Flight Updates to aircraft operators per year since 2009 to ensure consistent and reliable messaging is provided to Secure Flight stakeholders. Therefore, with respect to the Secure Flight program, we consider action complete.

TSA notes that this recommendation is based on findings cited in the report regarding initiatives (i.e., Known Traveler, TSA Pre✓™), which are TSA-wide initiatives under Risk-Based Security. Each of the pilot programs has a tailored communications strategy that evolves depending upon the results of the pilot program and decisions on system-wide implementation.

Again, thank you for the opportunity to review and comment on this report. The TSA Secure Flight program looks forward to working with OIG in the future.

Appendix D
Secure Flight Passenger Prescreening Process


Aircraft Operators Submit SFPD
Advance Flight Reservations
Changes to Flight Reservations
Last Minute Flight Reservations
Collect and Submit Full SFPD
DHS Traveler Redress Inquiry Program (TRIP) Cleared List
One DHS Solution
Secure Flight Automated Matching
OUTPUT
Error Messages: Incomplete or Invalid Passenger Data
Results Sent to Aircraft Operators
Cleared
Inhibited
VID
Selectee
Issue Boarding Pass
Aircraft Operator calls Secure Flight Operations Center
Do Not Board
Issue Boarding Pass with Selectee Designation

Source: Secure Flight Briefing, June 2011.

Appendix E
Major Contributors to This Report

Marcia Moxey Hodges, Chief Inspector
McKay Smith, Senior Inspector
Katherine Yutzey, Senior Inspector
Amy Tomlinson, Inspector
Heidi Einsweiler, Inspector

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Officer for Civil Rights & Civil Liberties
Chief Privacy Officer
Administrator, Transportation Security Administration
Commissioner, U.S. Customs and Border Protection
TSA Liaison
CBP GAO/OIG Liaison

U.S. Department of Justice

Director, Terrorist Screening Center
DOJ GAO/OIG Liaison

U.S. Department of Transportation

Administrator, Federal Aviation Administration
DOT GAO/OIG Liaison

Office of Management and Budget

Chief, Homeland Security Branch

DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or fax it directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.