Privacy Impact Assessment Update
for

Secure Flight

August 15, 2011

DHS/TSA/PIA-018(b)

Contact Point
Stacey Fitzmaurice
Director, Secure Flight Program
Transportation Security Administration
SFCommunications@dhs.gov

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Secure Flight program will match identifying information of aviation passengers and certain non-travelers against the No Fly and Selectee portions of the consolidated and integrated terrorist watch list and, if warranted by security considerations, other watch lists maintained by the federal government. The Transportation Security Administration (TSA) published a Final Rule and Privacy Impact Assessment (PIA) in October 2008,[1] outlining TSA's expected implementation of the Secure Flight program. This update reflects changes in the Secure Flight operational environment, as outlined below. Unless otherwise noted, the information provided in previously published PIAs remain in effect. Individuals are encouraged to read all program PIAs to have an understanding of TSA's privacy assessment of the Secure Flight program.

Introduction

The purpose of the Secure Flight program is to identify and prevent known or suspected terrorists or other individuals who may pose a threat to transportation security from boarding aircraft or accessing sterile areas[2] of airports where they may jeopardize the lives of passengers and others. The program is designed to better focus passenger and baggage screening efforts on passengers likely to pose a threat to civil aviation. Generally, the Secure Flight program will compare passenger and non-traveler information to the No Fly and Selectee List components of the Terrorist Screening Center Database. TSA, however, may use other watch lists maintained by TSA or other federal agencies to identify security risks when warranted by security considerations. A detailed discussion of the Secure Flight program may be found in previously published PIAs.

Reason for the PIA Update

This updated PIA addresses:

- <u>Conclusion of pre-operational test activities</u> TSA has concluded pre-operational test activities and all data collected prior to the implementation date of the Final Rule has been deleted from TSA systems.

---

[1] See Secure Flight Program PIA Update – DHS/TSA/PIA-018(a)
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf

[2] "Sterile area" is defined as a portion of airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under part 1544 of this chapter or a foreign air carrier under part 1546 of this chapter, through the screening of persons and property. 49 C.F.R. §1540.5.

- <u>Operators and Lessors of Twelve-Five aircraft</u> TSA will allow 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), to use Secure Flight to conduct watch list matching functions. In the future, TSA may mandate participation in Secure Flight by such charter and scheduled operators.

- <u>Centers for Disease Control and Prevention (CDC) Do Not Board List</u> TSA will compare passenger information against the identities of individuals whom the Department of Health and Human Services (HHS) CDC has identified to DHS as public health threats who should not be permitted to board an aircraft.

- <u>Customs and Border Protection (CBP) leveraging of Secure Flight communications infrastructure</u> In order to eliminate multiple messages to the airlines from CBP and TSA on a single passenger, Secure Flight will append and transmit the CBP's Electronic System for Travel Authorization (ESTA)[3] status code for international travelers to the Secure Flight boarding pass printing result.

- <u>Enhanced Security Screening</u> Secure Flight will incorporate an automated random selection process to select passengers for enhanced screening. Secure Flight will also transmit instructions to the airlines identifying individuals requiring enhanced screening derived from real-time threat-based intelligence scenarios run by the CBP Automated Targeting System[4] (ATS).

- <u>Airport Access Authorization to Commercial Establishments.</u> TSA currently permits airports to allow registered guests at hotels located on airport property to access commercial establishments (stores, restaurants) in the sterile area beyond the checkpoint. Guests must provide information to the airport operator for a check against watch lists used by Secure Flight.[5] TSA will permit airport authorities to leverage Secure Flight information technology infrastructure to perform Secure Flight checks on individuals (not limited to registered hotel guests) seeking access to commercial establishments in the sterile area beyond the checkpoint.

---

[3] Electronic System for Travel Authorization (ESTA) is an automated system used by CBP to determine the eligibility of visitors to travel to the United States under the Visa Waiver Program (VWP) and whether the traveler poses any law enforcement or security risk.

[4] For more information on ATS see the Privacy Impact Assessment for the Automated Targeting System, dated August 3, 2007 (Automated Targeting System Update – DHS/CBP/PIA-006(a) at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate10plus2.pdf).

[5] For more information, see the Privacy Impact Assessment for Airport Access Authorization to Commercial Establishments beyond the Screening Checkpoint, dated November 22, 2006.

- **Known Travelers** TSA incorporated into the Secure Flight program a capability to recognize known traveler programs. Known Travelers are individuals for whom the federal government has conducted a security threat assessment and determined does not pose a security threat. As an initial proof of concept, SF will recognize existing CBP Trusted Traveler programs[6] under which passengers can provide their Known Traveler number to Secure Flight for an appropriate boarding pass instruction. In the future, TSA may incorporate other populations within a Known Traveler concept, such as transportation sector workers who receive a TSA security threat assessment, and members of the military. Known Travelers may receive expedited screening, however, TSA reserves the right to incorporate random enhanced screening protocols within any Known Traveler program that Secure Flight will recognize.

- **Frequent Flyer programs** TSA will accept aircraft operator frequent flyer status codes for use in conjunction with risk-based security rules using Secure Flight Passenger Data (SFPD).[7] Secure Flight will accept a designator code signifying that the individual is a participant in a frequent flyer program for individuals who direct or permit that the information be provided to TSA. Frequent flyers may receive expedited screening, however, TSA reserves the right to incorporate random enhanced screening protocols.

Privacy Impact Analysis

Information Collected and Stored within the System

Operators and Lessors of Twelve-Five Aircraft

Section 4012 (a)(1)(E) of IRPTA requires DHS to permit charter operators and lessors of aircraft with a maximum takeoff weight in excess of 12,500 pounds to use Secure Flight to compare passengers and individuals seeking to charter or lease aircraft with a maximum takeoff weight greater than 12,500 pounds against the watch list.[8] TSA will also check these individuals

---

[6] See CBP Global Enrollment System PIA - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ges.pdf.

[7] SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), known traveler number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information.

[8] Public Law 108–458—Dec. 17, 2004; Intelligence Reform And Terrorism Prevention Act Of 2004. "Not later than 90 days after the date on which the Assistant Secretary assumes the performance of the advanced passenger prescreening function under subparagraph (C)(ii), the Assistant Secretary shall establish a process by which operators of aircraft to be used in charter air transportation with a maximum takeoff weight greater than 12,500 pounds and lessors of aircraft with a maximum takeoff weight greater than 12,500 pounds may request the Department of Homeland Security to use the advanced passenger prescreening system to compare information about any individual seeking to charter an aircraft with a maximum takeoff weight greater than 12,500 pounds, any passenger proposed to be transported aboard such aircraft, and any individual seeking to lease an aircraft with a maximum takeoff weight greater than 12,500 pounds to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government."

against lists maintained or used by TSA to identify risks to transportation or national security. While not covered by the Secure Flight Final Rule, TSA will allow such charter operators and lessors to use Secure Flight to perform these watch list matching functions. TSA will also permit scheduled operators under 49 CFR 1544.101(d) to participate. In the future, TSA may mandate participation by such charter and scheduled operators.

Aircraft operators and lessors of aircraft with a maximum takeoff weight in excess of 12,500 pounds will request that individuals who seek to charter, lease, or fly as passengers on such aircraft provide Secure Flight Passenger Data (SFPD)[9] to TSA for watch list matching.

For non-traveling individuals from whom the aircraft operator seeks authorization to enter an airport sterile area (such as to escort minors or passengers with disabilities), TSA requires the same information requested from passengers to be transmitted to TSA, in addition to certain non-personally identifiable information used to manage messages between covered aircraft operators and TSA, including the airport code for the sterile area to which the non-traveler seeks access.

<u>Centers for Disease Control (CDC) Do Not Board List</u>

Under section 361 of the Public Health Service Act (42 U.S.C. § 264), the CDC Director may apprehend, detain, examine, or conditionally release persons believed to be carrying certain communicable diseases that are specified in an executive order of the president. This list of diseases currently includes such diseases as cholera, diphtheria, infectious tuberculosis, plague, smallpox, yellow fever, viral hemorrhagic fevers (Lassa, Marburg, Ebola, Crimean-Congo, South American, and others not yet isolated or named), severe acute respiratory syndrome, and influenza caused by novel or re-emergent influenza viruses that are causing, or have the potential to cause, a pandemic. The CDC recommends that persons known to have communicable diseases that pose a serious public health threat, such as infectious tuberculosis, refrain from traveling by any public conveyance.

To address the risk to transportation or national security posed by exposure to these contagious diseases during air travel, the CDC partnered with the Department of Homeland Security (DHS) to prevent persons with diseases posing a serious public health threat from boarding commercial airline flights. Under this program, public health officials can request that CDC place persons who meet specific criteria and pose a serious threat to the public on a national public health Do Not Board list restricting them from boarding an aircraft. The public

---

[9] Full name, gender, date of birth, Redress Number (if available) or known traveler number (if implemented and available), passport information (if available), and certain non-personally identifiable information used to manage messages between covered aircraft operators and TSA, such as itinerary information for each passenger.

health Do Not Board list is managed by CDC and DHS, and is updated based on CDC notification to make additions, changes and deletions to the records contained within the list.

As discussed in the Secure Flight Final Rule, TSA worked with CDC to eliminate the unnecessary duplication effort from aircraft operators being required to independently check the Do Not Board list. TSA will compare passenger information against the identities of individuals who the CDC has identified to DHS and TSA via the Do Not Board list as public health threats who should not be permitted to board a commercial flight. Based on the CDC's identification, TSA prohibits air carriers from issuing boarding passes to these individuals because they pose a threat not only to passengers on a particular flight, but also to the transportation system should the disease spread to other flights and flight crew. The Secure Flight system does not retain health information.

Customs and Border Protection (CBP) leveraging of Secure Flight communications infrastructure

To facilitate the provision of a single matching result to the aircraft operator, TSA will append and transmit the Electronic System for Travel Authorization (ESTA) status code provided by CBP to the Secure Flight boarding pass printing result message. ESTA uses PII in determining the eligibility to travel of persons seeking to enter the United States under the Visa Waiver Program (VWP) by air or sea. ESTA will run the applicant's information against various databases to determine whether there is a law enforcement or security reason to deem that a prospective traveler is ineligible to travel to the United States under the VWP. For further information on ESTA, please consult the PIA.[10] TSA will not use the ESTA results as part of the Secure Flight determination, but will instead pass the result to the aircraft operator. This process reduces the burden on aircraft operators to manage multiple DHS responses and lessens the likelihood of errors that may occur from multiple transmissions.

Enhanced Security Screening

Secure Flight will transmit instructions identifying passengers who are selected by an automated random selection generator for enhanced screening. TSA will also leverage CBP's ATS to identify individuals requiring enhanced screening prior to boarding an aircraft. ATS uses current threat-based intelligence to identify passengers who may pose a greater risk for terrorist or criminal activity and are therefore subject to greater scrutiny. Secure Flight will transmit instructions identifying covered travelers requiring enhanced screening prior to boarding an aircraft derived from real-time threat-based intelligence scenarios run by CBP's ATS.

---

[10] See Electronic System for Travel Authorization (ESTA) – DHS/CBP/PIA-007(a) at
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_estafee_update.pdf

Airport Access Authorization to Commercial Establishments

Airports with approved Airport Security Plans permitting individuals to access commercial establishments located in the sterile area beyond the security checkpoint will use Secure Flight to perform watch list matching for those individuals. TSA will collect full name, gender, date of birth, Redress Number (if available) or Known Traveler number (if implemented and available), and passport information (if available).

Known Traveler and Frequent Flyer

TSA will collect the Known Traveler number and frequent flyer designator code.

Uses of the System and the Information

Operators and lessors of Twelve-Five aircraft

TSA will use SFPD to identify individuals who may pose a risk to transportation or national security. Operators and lessors of Twelve-Five aircraft may only use Secure Flight watch list results for aviation security purposes.

Centers for Disease Control (CDC) Do Not Board List

TSA will use SFPD to identify individuals who the CDC has nominated to the Do Not Board list and issue an appropriate boarding instruction to the aircraft operator.

Customs and Border Protection (CBP) leveraging of Secure Flight communications infrastructure

TSA receives the ESTA status code result from CBP for transmission to the aircraft operator. TSA will not use the ESTA status code as part of the Secure Flight program. TSA maintains only the ESTA code, not the underlying ESTA records.

Enhanced Security Screening

Secure Flight will use a random selection generator and ATS result for the purpose of identifying passengers for enhanced screening and issuing an appropriate boarding instruction to the aircraft operator.

Airport Access Authorization to Commercial Establishments

Information collected on individuals seeking access to commercial establishments located in the sterile area beyond the screening checkpoint will be used to perform Secure Flight watch list checks on those individuals. Participating airports are prohibited from using watch list match results for any other purpose.

Known Traveler and Frequent Flyer

TSA will use the Known Traveler number and frequent flyer designator code to issue an appropriate boarding pass instruction for expedited screening.

Retention

All data received by TSA as a part of pre-operational testing has been deleted in accordance with TSA's records disposition schedule approved by NARA General Records Schedule 20. The Secure Flight records retention schedule was approved by NARA in January 2009 (N1-560-08-3). That schedule provides for a retention period of 7 days for individuals who are not a match to a government watch list, 7 years for individuals who are a potential match to a government watch list, and 99 years for individuals who are a confirmed match to a government watch list. Changes reflected in this updated PIA are implemented within the existing schedule as follows:

Records associated with passengers and individuals seeking to charter or lease aircraft with a maximum takeoff weight greater than 12,500 pounds will be retained in accordance with the existing retention schedule.

Records of individuals on the CDC Do Not Board list or identified by ATS will be retained for 7 years. The Do Not Board list is updated based on requests from CDC to make additions, changes and deletions to the records contained within the list. TSA will amend its NARA-approved records retention schedule to reflect that confirmed CDC matches will be held for 7 years.

The retention period of records on individuals for whom Secure Flight receives an ESTA code will be based on the result of watch list checks. For example, records on an individual with an ESTA code, but who is not also a watch list match, will be held for no more than 7 days.

Records on individuals randomly selected by the automated selection generator will be based on the result of watch list checks. For example, an individual randomly selected for enhanced screening, but not also a watch list match, will be held for no more than 7 days.

The retention of records on individuals seeking access to airport commercial establishments located in the sterile area beyond the screening checkpoints will be based on the result of the watch list check. For example, individuals who are not a match to a watch list will be held for no more than 7 days.

The Known Traveler number will be retained with the Secure Flight Passenger Data and retained in accordance with existing NARA-approved records disposition based on the results of the watch list checks. If a Known Traveler is not on a watch list, the record will be retained no more than 7 days.

Internal Sharing and Disclosure

No changes.

External Sharing and Disclosure

No changes, except that in the event of potential matches to the CDC Do Not Board list that cannot be cleared through a manual review process by a Secure Flight analyst, TSA expects to share an individual's PII, Do Not Board list match result and analysis with HHS to adjudicate. TSA will also provide HHS with confirmed matches to the Do Not Board list. Sharing will be in person, in paper format, via facsimile, or by telephone, as required by the circumstances necessitating such sharing. This sharing is consistent with routine use 13 of the Secure Flight System of Records Notice (SORN), which states that TSA may share information with "appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, including the World Health Organization, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of communicable or quarantinable disease or for combating other significant public health threats; appropriate notice will be provided of any identified health threat or risk."[11] TSA may also notify aircraft and airport operators as necessary, depending on the health threat posed by the individual. This sharing is consistent with routine use 3 of the Secure Flight SORN which states that TSA may share information with "aircraft operators, foreign air carriers, airport operators and the Department of Transportation to communicate passenger watch list matching status and facilitate an operational response, where appropriate, to individuals who pose or are suspected of posing a risk to transportation or national security."

Notice

Passengers and individuals leasing or operating chartered Twelve-Five aircraft will be provided notice equivalent to that provided to existing populations covered by the Secure Flight Final Rule. Notice is provided electronically when reservations are made through websites and at self-service kiosks.

Individuals seeking to access commercial establishments in the sterile area beyond the security checkpoint will be provided with notice at the time their information is collected by the airport operator.

Frequent fliers will receive notice of the information collection from their aircraft operator and must authorize the aircraft operator to supply their frequent flyer status to TSA.

Known Travelers also will receive notice of the information collection and must supply their known traveler number to the aircraft operator to provide to TSA.

---

[11] The Secure Flight SORN can be found at 72 F.R. 63711

Individual Access, Redress, and Correction

If an individual believes he or she has improperly been denied entry, refused boarding for transportation, or identified for additional screening due to their ESTA status or enhanced security screening results, that individual may seek redress through the DHS Traveler Redress Program ("TRIP").[12] Individuals randomly selected for Enhanced Security Screening may seek redress through TRIP but there will not be an underlying condition susceptible to redress or correction.

If an individual believes he or she has been wrongly placed on the CDC Do Not Board list, that individual may contact their local health official/doctor responsible for contacting the CDC about their condition or HHS.

Technical Access and Security

The Secure Flight system has completed the certification and accreditation processes and received its Authority to Operate (ATO) on March 31, 2010.

Technology

No update.

Responsible Official

Stacey Fitzmaurice, Director Secure Flight
Transportation Threat Assessment and Credentialing
Transportation Security Administration
Department of Homeland Security

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

---

[12] http://www.dhs.gov/files/publications/gc_1282922720391.shtm#002