



**Privacy Impact Assessment Update
for**

Secure Flight

DHS/TSA/PIA-018(e)

April 13, 2012

Contact Point

Stacey Fitzmaurice

Director, Secure Flight Mission Support Branch

Transportation Security Administration

SFCommunications@dhs.gov

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Transportation Security Administration (TSA) Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas¹ or board aircraft.² This screening compares these individuals to the No Fly and Selectee portions of the consolidated and integrated terrorist watch list, against other watch lists maintained by the federal government when warranted by security considerations,³ and against a list of passengers with redress numbers, *i.e.*, passengers who have been assigned a unique number by the Department of Homeland Security (DHS) Traveler Redress Inquiry Program (TRIP).⁴ In August 2011, TSA updated the Secure Flight PIA to reflect a number of changes, including:

1. the initiation of a Known Traveler proof of concept starting with individuals enrolled within Customs and Border Protection (CBP) Trusted Traveler programs, and expected to expand to include other populations such as transportation sector workers receiving TSA security threat assessments and members of the military; and
2. the receipt by Secure Flight of aircraft operator frequent flyer status⁵ codes for use in conjunction with risk-based security rules using Secure Flight Passenger Data (SFPD).

This PIA update reflects the transition from proof of concept to operational program of the Known Traveler and frequent flyer concepts within a program known as TSA Pre✓™. In addition to the populations noted above, TSA intends to initiate new pilot programs designed to test the expansion of the Known Traveler program to other populations, such as eligible members of the U.S. Armed Forces and certain active security clearance holders. In addition, TSA will create, maintain, and screen against a watch list of individuals who, based upon their involvement in violations of security regulations of sufficient severity or frequency, are disqualified from receiving expedited screening for some period of time or permanently.

This PIA Update further provides updated information on TSA's use of CBP's Automated Targeting System (ATS). Unless otherwise noted, the information provided in

¹ "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.

² In October 2008, the TSA published the Secure Flight Final Rule (73 Fed. Reg. 64018, Oct. 28, 2008) and the related PIA (Secure Flight Program PIA Update – DHS/TSA/PIA-018(a) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf).

³ Secure Flight also checks against the Center for Disease Controls Do Not Board list for public health threats, as discussed more fully in the August 2011 PIA Update.

⁴ In October 2008, the Transportation Security Administration (TSA) published the Secure Flight Final Rule (73 Fed. Reg. 64018, Oct. 28, 2008) and the related Privacy Impact Assessment (PIA) (Secure Flight Program PIA Update – DHS/TSA/PIA-018(a) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf).

⁵ This "status code" is referred to herein as the frequent flyer "designator code."



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 screen individuals before they access airport sterile areas or board aircraft. Generally, this screening has been designed to identify and prevent known or suspected terrorists or other individuals from gaining access to airports and airplanes where they may jeopardize the lives of passengers and others. To identify those who present a threat to aviation security, the Secure Flight program⁶ compares passenger and non-traveler information to the No Fly and Selectee List components of the Terrorist Screening Center Database (TSDB)⁷ and, when warranted by security considerations, other watch lists maintained by TSA or other federal agencies. Secure Flight also screens passengers against a list of passengers with redress numbers assigned by DHS TRIP, and against the list of individuals whom the Department of Health and Human Services Centers for Disease Control and Prevention (CDC) has identified to DHS as persons who should not be permitted to board an aircraft due to public health concerns.

With the proof of concept program announced in the August 2011 Secure Flight PIA Update⁸, TSA began to test the use of a largely dormant aspect of the Secure Flight program—the Known Traveler feature—to identify those individuals for whom expedited screening may be appropriate. TSA also announced that Secure Flight would accept frequent flyer designator codes for use in conjunction with risk-based security rules using SFPD. By reducing the screening resources at airports devoted to these trusted travelers, TSA will be able to focus its screening efforts on passengers who are more likely to pose a threat to civil aviation.

Reason for the PIA Update

This updated PIA reflects the establishment of the TSA Pre✓™ program and its interaction with Secure Flight. TSA Pre✓™ will incorporate the proof of concept Known Traveler program identified in the August 2011 PIA Update in which TSA recognizes existing CBP Trusted Traveler programs⁹ and eligible members of the U.S. Armed Forces for expedited screening (while reserving the right to incorporate random enhanced screening protocols). TSA is exploring the feasibility of expanding the Known Traveler program beyond these populations to include groups such as certain active security clearance holders, aviation workers and other transportation sector populations for whom TSA performs a security threat assessment, and other

⁶ A detailed discussion of the Secure Flight program may be found in previously published PIAs.

⁷ For additional information about the TSDB, see http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs.

⁸ Secure Flight Program PIA Update – DHS/TSA/PIA-018(b) <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-secure-flight.pdf>

⁹ See CBP Global Enrollment System PIA - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ges.pdf.



populations. This PIA will be updated as TSA incorporates new Known Traveler populations into the Secure Flight program.

With regard to the use of Frequent Flyer designator codes, this updated PIA reflects that Secure Flight will include as a data element the aircraft operator frequent flyer designator code¹⁰ for use in conjunction with SFPD.¹¹ Secure Flight will collect a designator code from participating aircraft operators for the purpose of verifying that a passenger is a Frequent Flyer program member eligible for expedited screening (subject to random enhanced screening protocols).

This PIA update also provides notice that, as part of the TSA Pre✓™, TSA will create and maintain a watch list of individuals who are disqualified from receiving expedited screening for some period of time or permanently because they have been involved in violations of security regulations of sufficient severity or frequency (the TSA Pre✓™ Disqualification List). Disqualifying violations of aviation security regulations may involve checkpoint and checked baggage violations, such as a loaded firearm that is discovered in carry-on baggage at the checkpoint.

As discussed in the August 2011 PIA update, TSA leverages CBP's ATS¹² to identify individuals requiring enhanced screening prior to boarding an aircraft. This PIA update provides notice that under this process, TSA creates and provides risk-based, intelligence-driven, scenario rules to CBP for use in ATS to identify international travelers requiring enhanced screening. TSA receives from CBP a continuously updated watch list of these individuals for use in Secure Flight. Certain intelligence-driven scenario rules may result in some travelers receiving enhanced screening for subsequent domestic and international flights for a period of time. Oversight will be exercised by DHS Privacy, DHS Office for Civil Rights and Civil Liberties, and DHS Office of General Counsel to ensure that the threat-based intelligence is appropriately applied.

¹⁰ The designator code is not the same as a Frequent Flyer number or the name of the aircraft operator. It is a separate and unique number assigned by TSA to each participating aircraft operator.

¹¹ 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.

¹² ATS uses current threat-based intelligence to identify passengers who may pose a greater risk for terrorist and are therefore subject to greater scrutiny.



Privacy Impact Analysis

Information Collected and Stored within the System

Collection at Reservation

When making a travel reservation, individuals participating in TSA Pre✓™ will provide aircraft operators the number associated with the program that qualifies them for TSA Pre✓™, along with their name, gender, and date of birth, which will then be provided to for use in Secure Flight as part of the SFPD. Additionally, TSA will collect from participating aircraft operators the frequent flier designator code described above for eligible Frequent Flier program participants.

Storage of Known Traveler Information

TSA will maintain lists of individuals with Known Traveler numbers eligible for expedited screening within the Secure Flight computer system. Secure Flight will check against these lists before issuing a boarding pass printing instruction. Secure Flight will maintain name, gender, date of birth, citizenship, and assigned number for eligible CBP Trusted Travelers. Secure Flight will maintain date of birth and an assigned number for eligible security clearance holders that is unique to TSA Pre✓™. For eligible members of the U.S. Armed Forces, Secure Flight will maintain name, gender, date of birth, and the Common Access Card number.

Collection of Watch List Information

For individuals identified through TSA's use of ATS discussed above, Secure Flight will receive from CBP and store a watch list of individuals requiring enhanced screening that will be updated to reflect the addition or deletion of individuals, as warranted.

Secure Flight also will receive and store a watch list of individuals who have been disqualified from receiving expedited screening due to violations of aviation security regulations. This TSA Pre✓™ Disqualification List will contain the name, gender, date of birth, and identifying number (if available) of disqualified individuals. The TSA Pre✓™ Disqualification List will be updated, as warranted, to reflect the addition or deletion of individuals.

Risks

Privacy risks associated with collecting and storing the lists of eligible Known Travelers, the list of individuals identified through the use of ATS, and the TSA Pre✓™ Disqualification List are mitigated through restrictions on the use and dissemination of the lists. In addition, privacy risks for CBP Trusted Travelers are low because the data already are maintained within DHS for similar expedited travel screening purposes. Privacy risk for individuals within the U.S. Armed Forces list is mitigated through the notice provided by the amendment by the Department



of Defense of its applicable System of Records Notice¹³ to expressly identify its sharing with TSA. Finally, privacy risks for eligible security clearance holders is mitigated by collecting information that is so limited (only a number and date of birth) that it cannot be used for any other purpose. Privacy risks associated with collecting and storing the frequent flyer designator code are the same as the risks associated with collection and storage of SFPD.¹⁴

Uses of the System and the Information

TSA will use the Known Traveler data and the frequent flyer designator code data collected by Secure Flight, as well as the watch list generated from CBP's ATS and the TSA Pre✓™ Disqualification List, to issue an appropriate boarding pass instruction for screening.

Retention

TSA will retain lists of Known Travelers which will be updated as needed to reflect the addition or deletion of individuals. In addition, the list of individuals identified through ATS will be retained within TSA Office of Intelligence & Analysis for no longer than two years. TSA intends to amend its NARA-approved records retention schedule for the Office of Intelligence & Analysis to reflect this change. Records will be retained until the amended records retention schedule is approved by NARA.

Internal Sharing and Disclosure

Information about individuals on the watch list generated by CBP's ATS and on the TSA Pre✓™ Disqualification List will only be shared internally for oversight, redress, and litigation purposes.

External Sharing and Disclosure

Information about individuals on the watch list generated by CBP's ATS and on the TSA Pre✓™ Disqualification List will not be shared externally unless the individual is involved in a security incident or is also on the TSDB or other watch lists. Information on individuals eligible to receive expedited screening will not be shared unless the individual is involved in a security incident or pursuant to 5 U.S.C. § 552a(b)(7).

Notice

TSA identified the potential for Known Travelers as part of the public rule-making associated with the Secure Flight program in 2007. TSA receives information on eligible TSA Pre✓™ participants either with the consent of the individual or pursuant to the Privacy Act, 5

¹³ Defense Enrollment Eligibility Recording System (DEERS), (Aug. 3, 2011, 76 FR 46757) <http://dpclo.defense.gov/privacy/SORNs/component/osd/DMDC02.html>

¹⁴ These risks are addressed in the original Secure Flight PIA.



U.S.C. § 552a, through an internal sharing or a published routine use from another federal government agency's System of Records Notice. Participants in the CBP Trusted Traveler programs were notified of their eligibility for TSA Pre✓™ by CBP as well as by media announcements. This PIA also serves as notice to the public and TSA will publish an update to the Secure Flight System of Records Notice.

Individual Access, Redress, and Correction

Individuals who are disqualified from expedited screening due to violations of security regulations have an opportunity to challenge the underlying violation that led to the disqualification through TSA's established administrative process for civil penalties. Individuals who believe they have been misidentified on the TSA Pre✓™ Disqualification List and/or the watch list generated by CBP's ATS may seek redress through DHS TRIP.

Technical Access and Security

No change.

Technology

The status of eligible members of the U.S. Armed Forces is currently confirmed in pilot program efforts through electronic readers provided by the DoD that verify the individual's status through a simple green/red light. The readers do not provide system connections between Secure Flight and the DoD systems. For operational reasons, it is not expected that the electronic readers will be deployed as a long-term solution for DoD participants in TSA Pre✓™.

Responsible Official

Stacey Fitzmaurice
Director Secure Flight Mission Support Branch
Office of Intelligence and Analysis
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