Privacy Impact Assessment
for the

Secure Flight Program

August 9, 2007

Contact Point
Peter Pietra
Privacy Officer
Transportation Security Administration
TSAPrivacy@dhs.gov

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Secure Flight program is intended to match identifying information of aviation passengers and certain non-travelers against the consolidated and integrated terrorist watch list maintained by the Federal Government[1] in a consistent and accurate manner, while minimizing false matches and protecting personally identifiable information. The Transportation Security Administration (TSA) is publishing a Notice of Proposed Rulemaking (NPRM) proposing TSA's implementation of the Secure Flight program. In conjunction with this NPRM, TSA is publishing this Privacy Impact Assessment (PIA), a Privacy Act System of Records Notice (SORN) and an NPRM proposing Privacy Act exemptions. This PIA reflects the Secure Flight program as proposed in the NPRM. The program and this PIA are expected to change in response to public comment on the NPRM. A revised PIA and if necessary a revised SORN will be issued in conjunction with the Final Rule for Secure Flight.

Introduction

The purpose of the Secure Flight program is to identify and prevent known or suspected terrorists 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. In addition, the Secure Flight program is intended to facilitate the secure and efficient travel of the vast majority of the traveling public while protecting individuals' privacy.

TSA is proposing to implement the Secure Flight program in accordance with section 4012(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004). Under the Secure Flight program, TSA intends to collect limited Secure Flight Passenger Data (SFPD) from certain U.S. aircraft operators and foreign air carriers for the purpose of passenger watch list matching against the No Fly and Selectee list components of the Terrorist Screening Database. SFPD consists of full name, date of birth, gender, redress number[3] (if available), known traveler number[4] (if implemented and available), and passport information[5] (if available).

---

[1] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) § 4012(a) (Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004). Currently, the consolidated and integrated terrorist watch list is maintained by the Federal Bureau of Investigation's Terrorist Screening Center (TSC) in the Terrorist Screening Database (TSDB). The No Fly and Selectee List are components of the TSDB.

[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.

[3] A redress number would be a unique number assigned to individuals who use the proposed redress process for Secure Flight that the individual may use in future correspondence with DHS and when making future travel reservations.

[4] A known traveler number would be 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.

[5] Passport information consists of passport number, country of issuance, expiration date, gender, and full name.

Pursuant to this authority, TSA is issuing this PIA, a SORN, an NPRM proposing Privacy Act exemptions, and associated NPRM for the Secure Flight program, under which TSA would receive passenger and certain non-traveler information from aircraft and airport operators, conduct watch list matching, and transmit boarding pass printing instructions back to aircraft and airport operators. As part of the implementation of the Secure Flight program, TSA would conduct operational testing of its capabilities to interact with and perform matching of names to the consolidated and integrated terrorist watch list maintained by the Federal Government[6] for each covered aircraft operator[7] before assuming the watch list matching function from each aircraft operator. Although covered aircraft operators would be required to conduct operational testing with TSA after the final rule is effective, covered aircraft operators may voluntarily choose to begin testing with TSA prior to the publication or effective date of the final rule. The consolidated and integrated terrorist watch list is maintained by the Federal Bureau of Investigation's Terrorist Screening Center (TSC) in the Terrorist Screening Database (TSDB).[8] The No Fly and Selectee List are components of the TSDB.

Current Watch List Matching Process

TSA currently performs passenger and baggage screening at the nation's commercial airports (*See* 49 U.S.C. 44901). Additionally, aircraft operators conduct passenger watch list matching using the No Fly and Selectee list components of the TSDB, and as required under security directives TSA issued following the terrorist attacks of September 11, 2001. Aircraft operators also conduct this watch list matching process for non-traveling individuals authorized to enter the sterile area of an airport in order to escort a passenger or for some other purpose approved by TSA.

Under the current watch list matching process conducted by the aircraft operators, when an aircraft operator has a passenger reservation in a name that is the same as, or similar to, a name on the No Fly List, the aircraft operator is required to notify law enforcement personnel and TSA in order to determine whether that passenger is in fact the individual whose name is on the No Fly List. If the passenger is verified as an individual on the No Fly List, the aircraft operator is prohibited from transporting the passenger. When an aircraft operator has a passenger reservation in a name that is on the

[6] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) § 4012(a) (Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004).

[7] U.S. aircraft operators that are required to have a full security program under 49 CFR 1544.101(a) and foreign air carriers that are required to have a security program under 49 CFR 1546.101(a) or (b). These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports. In the NPRM they are referred to as "covered U.S. aircraft operators" and "covered foreign air carriers" respectively, and collectively as "covered aircraft operators."

[8] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated and integrated terrorist watch list, known as the TSDB.

Selectee List, the aircraft operator is required to identify the individual to TSA for enhanced screening at security screening checkpoints.[9]

Watch List Matching Process Proposed Under Secure Flight

The Secure Flight program implements a mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec. 17, 2004) and is consistent with TSA's authority under the Aviation and Transportation Security Act (ATSA). Section 4012(a)(1) of the IRTPA requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the Federal Government. Section 4012(a)(2) of IRTPA similarly requires DHS to compare passenger information for international flights to and from the United States against the consolidated and integrated terrorist watch list before departure of such flights..

For passengers on covered flights, TSA is proposing to require covered aircraft operators to request passengers' full name, gender, date of birth, and Redress Number (if available) or known traveler number (if implemented and available). Passengers must provide their full name. Covered aircraft operators would then be required to transmit to TSA the Secure Flight Passenger Data (SFPD), which contains the information provided by each passenger, as well as passport information (if available), and certain non-personally identifiable information used to manage messages between covered aircraft operators and TSA, including itinerary information, for each passenger.

For non-traveling individuals for whom the aircraft operator seeks authorization to enter an airport sterile area (such as to escort minors or passengers with disabilities), TSA also is proposing to require covered aircraft operators to request from the non-traveler the same information requested from passengers and transmit to TSA that information as well as 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.

Generally, the Secure Flight program will compare passenger and non-traveler information to the No Fly and Selectee List components of the TSDB, which are currently used for the pre-flight passenger watch list matching conducted by aircraft operators. However, as recommended in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), TSA may use the "larger set of watch lists maintained by the Federal government."[10] Therefore, pursuant to 49 U.S.C. § 114(f) which requires TSA to assess threats to transportation, where warranted by security considerations, TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases. For example, TSA may obtain intelligence that flights flying a particular route may be subject to an increased security risk. Under this circumstance, TSA may decide to compare passenger information on some or all of the flights flying that route against the full TSDB or other government databases. The watch list matching process against the No Fly and Selectee list components of the TSDB, supplemented with additional checks where warranted by security considerations, will be referred to as "watch list matching".

[9] Individuals may undergo enhanced screening at security screening checkpoints for a variety of other reasons, such as random selection or a walk through a metal detector alarm.

[10] National Commission on Terrorist Attacks Upon the United States, page 393.

Based on the watch list matching results produced by Secure Flight (using either the No Fly and Selectee List or the full TSDB or other government databases where warranted by security considerations), TSA would instruct an aircraft operator to process the individual in the normal manner, to identify the individual for enhanced screening at a security checkpoint, or to deny the individual transport or authorization to enter the airport sterile area.

TSA is proposing to retain records for most individuals encountered by Secure Flight for a short period of time. Records for individuals who are not identified as potential matches by the automated matching tool, which comprise the vast majority of travel records held by TSA, would be retained for seven (7) days after the completion of the individual's directional travel for audit purposes. Records for individuals who are potential or confirmed matches would be retained for no less than seven years after the completion of the individual's directional travel, as outlined in section 3.0 of this PIA. These records would be available if needed as part of the redress process discussed in section 7.0 of this PIA. In case of a terrorist event, records concerning the event, which may possibly include passenger information, would be retained in accordance with a separate TSA record retention schedule covering major security incident records. This information would be retained to support the investigation and documentation of a terrorist event. Such records would be maintained in accordance with applicable SORNs, DHS/TSA 001, Transportation Security Enforcement Records System, 69 Fed. Reg. 71818, 71829 (December 10, 2004) and DHS/TSA 011, Transportation Security Intelligence Service Operations Files, 69 Fed. Reg. 71828, 71835 (December 10, 2004).

Scope

The Secure Flight NPRM would affect U.S. aircraft operators that are required to have a full program under 49 CFR 1544.101(a) and foreign air carriers that are required to have a security program under 49 CFR 1546.101(a) or (b). These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports. They are referred to in the associated NPRM as "covered U.S. aircraft operators" and "covered foreign air carriers" respectively, and collectively as "covered aircraft operators." Under the NPRM, the program would eventually cover all flights conducted by covered U.S. aircraft operators, and all flights conducted by a covered foreign air carrier arriving in or departing from the United States, or overflying the continental United States. These flights are referred to in the NPRM as "covered flights."

Implementation Stages of Secure Flight

TSA proposes to implement this rule in two stages where the first stage would include covered flights between two domestic points in the United States and the second stage would include covered flights to or from the United States, flights that overfly the continental United States, and all other flights (such as international point to point flights) operated by covered U.S. aircraft operators not covered in the first stage.

During the first stage of implementation, TSA would assume the watch list matching function for domestic flights conducted by covered U.S. aircraft operators. During the second phase, TSA is proposing to begin watch list matching for all other flights operated by covered U.S. aircraft operators, as well as covered flights operated by covered foreign air carriers. Customs and Border Protection (CBP) currently requires covered foreign air carriers to collect and transmit passenger information to CBP for

border enforcement purposes as well as watch list matching prior to the departure of a flight under its Advance Passenger Information System (APIS) pre-departure final rule. As part of the second stage of Secure Flight implementation, TSA would assume the watch list matching function for covered foreign air carriers from CBP.

Pursuant to the associated NPRM, TSA will also conduct passenger watch list matching for passengers on flights that fly over the United States during the second phase of implementation, except for those flights that transit the airspace of the United States between two airports or locations in the same country, where that country is Canada or Mexico.

Privacy Documentation

In conjunction with the NPRM for the Secure Flight Program, TSA is publishing this PIA, a Privacy Act SORN and an NPRM proposing Privacy Act exemptions. This PIA and the associated SORN address both implementation stages of the Secure Flight Program. TSA will issue an amended PIA and a revised SORN in conjunction with the Secure Flight Final Rule as necessary. Although not required, covered aircraft operators may voluntarily choose to begin operational testing with TSA prior to publication of a Final Rule. This PIA and the associated SORN would cover any testing between an aircraft operator and TSA including both domestic and international flights prior to the publication of or effective date of the Final Rule, and cover required operational testing. TSA will also amend the PIA in the event TSA issues a rulemaking to extend the Secure Flight program to cover watch list matching for other categories of aircraft operators, such as public or private charter flight operators.

Section 1.0

Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

Airlines currently collect information from passengers and non-travelers that is necessary both for security purposes and for ensuring passenger comfort during their flights to their destinations.

Under the Secure Flight NPRM, TSA would require covered aircraft operators to send to TSA Secure Flight Passenger Data (SFPD) that will consist of the below listed elements, to the extent available.

(1) full name;

(2) date of birth;

(3) gender;

(4) redress number (if available);

(5) known traveler number (if implemented and available); and

(6) passport information (if available).

To manage the processing of the SFPD, TSA will require aircraft operators to include in the SFPD the following information: Reservation Control Number; Record Sequence Number; Record Type; Passenger Update Indicator; Traveler Reference Number; and Itinerary information.

Covered aircraft operators would be required to request from passengers or non-traveling individuals their full name, date of birth, gender, and redress number or known traveler number. Individuals must provide their full names in order to make a reservation or request authorization to access a sterile area but are not required to provide the other data elements requested. Although covered aircraft operators would not be required to ask for passport information for individuals traveling on domestic flights, covered aircraft operators would be required to transmit the passport information if they collect such information in the ordinary course of business. It should be noted that passport information is not required to travel domestically. For passengers who have reserved an international flight but who have not yet traveled on an international flight as part of their travel itinerary, covered aircraft operators would collect passport information in accordance with CBP regulations and would be required under this proposed rule to transmit such information to TSA as soon as it is available.

A covered aircraft operator may, in the ordinary course of business and as part of its reservation process, input data that TSA requires covered aircraft operators to request from individuals, but that the individual did not provide at the time of reservation, such as data from a passenger profile stored by the aircraft operator. In these situations, the aircraft operator would be required to include that data as part of the SFPD transmitted to TSA to assist with effective automated watch list matching. Any data elements sent by the covered aircraft operator in addition to those required by TSA would be automatically filtered out prior to submission to the Secure Flight system to ensure that Secure Flight does not receive any nonessential information.

At a future date, covered aircraft operators may be required to begin accepting known traveler numbers from Federal programs approved for use by TSA. TSA will inform covered aircraft operators in writing of the date on which they must begin to request an approved category of known traveler numbers. TSA expects that the covered aircraft operator would request this information from the individual making a reservation on a covered flight or requesting access to a sterile area of an airport. The covered aircraft operator would then be required to enter known traveler information provided by the passenger into the SFPD. If TSA begins accepting known traveler numbers, it will only be necessary to include one reference number in a SFPD. That reference number could be a redress number or a known traveler number.

Proposed Information Collection Requirements for Secure Flight

Data Elements	Covered Aircraft Operators Must Request from Passengers	Passengers Must Provide	Covered Aircraft Operators Must Transmit to TSA
Full Name	X	X	X
Date of Birth	X		If available[11]
Gender	X		If available
Redress Number or Known Traveler Number	X		If available
Passport Information			If available[12]
Itinerary Information[13]			X
Reservation Control Number			X
Record Sequence Number			X
Record Type			X
Passenger Update Indicator			X

TSA may be unable to complete the watch list matching process for an individual if the individual fails to provide information sufficient to distinguish him or her from an individual who appears on the watch list. The proposed rule provides that if TSA cannot determine from the information provided by the covered aircraft operator whether an individual is a match to the watch list prior to the individual's arrival at the airport or online check-in, it will be necessary for the individual to provide additional information at the airport. These individuals may be asked to present to the covered aircraft operator a verifying identity document, which must be unexpired, issued by a Government (Federal, State, local, or tribal), and contain the individual's full name, photo, and date of birth. An unexpired passport issued by a foreign government would also constitute a verifying identity document.

Once the individual provides a verifying identity document to the covered aircraft operator, the proposed rule would require the aircraft operator to update the passenger's SFPD with any of the missing and/or incomplete data elements from the list described previously and transmit to TSA the additional information from the individual's verifying identity document. There may be occasions where the aircraft operator will need to call TSA. In such cases, the aircraft operator may be asked to provide additional identifying information about the passenger, such as a physical description, that may be required by TSA to complete the watch list matching process. Secure Flight may retain some of the additional information

[11] "If available" means: (1) data provided by the passenger at the time of reservation; (2) data provided by the passenger at the ticket counter; or (3) data that TSA requires covered aircraft operators to request from individuals, but that the individual did not provide at the time of reservation, such as data from a passenger profile stored by the aircraft operator.

[12] Passport information is not required to travel domestically.

[13] Itinerary information includes the following information about a covered flight: (1) departure airport code; (2) aircraft operator; (3) departure date; (4) departure time; (5) arrival airport code; (6) flight number; (7) operating carrier (if available). For non-traveling individuals, itinerary information includes the airport code for the sterile area to which the non-traveling individual seeks access.

about the passenger in accordance with the proposed retention schedule discussed in section 3.0 of this PIA. TSA will complete the watch list matching process, in coordination with the TSC, and provide the aircraft operator with boarding pass printing instructions for that individual.

1.2 What are the sources of information in the system?

Aircraft operators will request the information outlined above from passengers and non-traveler individuals requesting access to airport sterile areas.

The term "passenger" references an individual who has, or seeks to obtain, a reservation for transport on a domestic flight operated by a covered U.S. aircraft operator. The proposed definition of "passenger" will exclude any crew member traveling on duty and any individual with flight deck privileges under 49 CFR 1544.237 who is traveling on the flight deck as these individuals already undergo a security threat assessment as required by TSA. The definition includes an employee who is not on duty but who is accommodated in a "jump seat" in the cabin.

"Non-traveling individual" or "non-traveler" refers to an individual to whom the covered U.S. aircraft operator or covered airport operator seeks to issue an authorization to enter the sterile area of an airport in order to escort a minor or disabled passenger or for some other purpose permitted by TSA. "Non-traveling individual" does not include employees or agents of airport or aircraft operators or other individuals whose access to a sterile area is governed by another TSA regulation or security directive.

"Covered aircraft operators" refer to all U.S. aircraft operators who conduct certain covered flights operating within the United States. A second phase of the program will expand to include international flights operated by U.S. aircraft operators and flights operated by foreign air carriers into, out of and over the United States. In implementing Secure Flight, TSA anticipates that it will begin assuming the watch list matching function from covered U.S. aircraft operators first.

Additionally, Secure Flight receives information from the Terrorist Screening Center's Terrorist Screening Database No Fly and Selectee lists. Pursuant to 49 U.S.C. § 114(f), where warranted by security considerations, TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases. For example, TSA may obtain intelligence that flights flying a particular route may be subject to an increased security risk. Under this circumstance, TSA may decide to compare passenger information on some or all of the flights flying that route against the full TSDB or other government databases.

1.3 Why is the information being collected, used, disseminated, or maintained?

As required under section 4012 of the IRTPA, TSA will obtain passenger and non-traveler information in order to assume the function of conducting watch list comparisons. Based on the watch list matching results, an aircraft operator will be provided with boarding pass printing instructions necessary to perform one of three functions: (1) process the individual in the normal manner; (2) identify the individual for enhanced screening at a security checkpoint; or (3) deny the individual transport or authorization to enter the airport sterile area. Pursuant to 49 U.S.C. § 114(f), where warranted by security

considerations TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases, where warranted by security considerations.

Before TSA assumes the watch list matching function from each aircraft operator, passenger and non-traveler information will be collected and submitted to Secure Flight during operational testing with each aircraft operator. Operational testing will be conducted to test the transmission connections between Secure Flight and each covered aircraft operator and to test Secure Flight's ability to receive passenger and non-traveler information, conduct watch list matching, and transmit boarding pass printing instructions back to the aircraft operator. Operational testing will allow TSA to refine program operations and verify its ability to effectively conduct watch list matching before TSA assumes the function from aircraft operators. After TSA successfully completes operational testing with aircraft operators, TSA will begin the process (including DHS certification and Congressional reporting as required by statute) to assume the watch list matching function from aircraft operators.

1.4 How is the information collected?

Airport operators and aircraft operators will collect passenger and non-traveler information by electronic means or verbally.

TSA is proposing to require covered aircraft operators to transmit SFPD to TSA prior to flight departure time, in accordance with each aircraft operator's Aircraft Operator Implementation Plan (AOIP). TSA anticipates requiring covered aircraft operators to transmit SFPD to TSA approximately 72 hours prior to scheduled flight departure time for reservations made 72 hours or more before the scheduled departure time of the flight. For reservations made within 72 hours of scheduled flight departure time, TSA anticipates requiring covered aircraft operators to transmit the SFPD immediately after the reservation is made.

Covered aircraft operators that voluntarily choose to begin operational testing with TSA prior to publication of a Final Rule will provide SFPD to TSA via secure means as agreed to by the aircraft operators and TSA.

Covered aircraft operators would be required to accurately transmit passenger and non-traveler SFPD. However, covered aircraft operators would not be required to validate the underlying accuracy of the collected passenger or non-traveler information. Covered aircraft operators would be required to transmit information updates to reflect changes to any information required in the SFPD. TSA is working with other agencies, including CBP, to develop ways to eliminate unnecessary duplication of comparable screening efforts and thereby reduce governmental and private sector costs.

1.5 How will the information be checked for accuracy?

The Secure Flight system will rely on the following measures to promote the accuracy of the information it utilizes:

- The accuracy of SFPD transmitted to TSA by the aircraft operators will be initially based on the accuracy of passenger and non-traveler information submitted by the individual at the time of airline reservation.

- Personal information that changes after initial transmission to TSA due to passenger or covered aircraft operator reservation modifications will be re-transmitted by covered aircraft operators to Secure Flight.
- Name, date of birth, and gender may be verified at the aircraft operator ticket counter if an individual is identified as a possible match to the watch list that would warrant denying issuance of a boarding pass. Data verification will validate whether the submitted SFPD is consistent with the passenger's government-issued identification.
- Additional identifying information provided through the resolution process while the passenger is at the ticket counter may be reviewed by Secure Flight analysts to help resolve reasonably similar or exact matches to names on the watch list.
- The system generates and maintains data quality metrics which will be used to identify problematic trends for remediation.
- The redress process described in Section 7.0 below is a mechanism to maintain and improve accuracy of information.

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

TSA's general operating authorities are set forth in the Aviation and Transportation Security Act (ATSA) 49 U.S.C. § 114(f). IRTPA specifically directs TSA to test and implement a pre-flight watch list matching program, such as Secure Flight. Section 4012(a)(1) of the IRTPA requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the Federal Government. Section 4012(a)(2) of IRTPA similarly requires the DHS to compare passenger information for international flights to, from the United States against the consolidated and integrated terrorist watch list before departure of such flights. Pursuant to 49 U.S.C. § 114(f), TSA is required to assess threats to transportation. Therefore, in addition to current checking of the No Fly and Selectee watch lists, where warranted by security considerations, TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases, where warranted by security considerations.

1.7 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

In connection with its information collection activities, TSA seeks to implement Fair Information Practices, including minimization of data collection. TSA has limited the proposed information collection requirements for Secure Flight to the data elements TSA believes are minimally necessary for effective watch list matching of aviation passengers. In making this determination, TSA has attempted to balance the privacy interest in minimizing the collection of personal information with the need to conduct effective watch list matching to protect the security of the United States and to avoid unnecessarily delaying legitimate passengers due to misidentification.

TSA has determined that an individual's full name, gender, and date of birth are critically important for effective automated matching of that individual against those individuals on the watch list. Full name is the primary attribute used to conduct watch list matching. Many names, including non-

English names, do not indicate gender because they can be used by either gender. Additionally, names not derived from the Latin alphabet, when transliterated into English, often do not denote gender. Providing information on gender will reduce the number of false positive watch list matches because the information will distinguish persons who have the same or similar names but who are of different gender.

Similarly, date of birth is helpful in distinguishing a passenger from an individual on a watch list with the same or similar name, thereby reducing the number of false positive watch list matches. (By way of example only, Pat born 12/10/1976 may be less likely to be matched with Patrick born 12/1/1967 with the addition of gender and date of birth.)

TSA has determined that passport information would enable TSA analysts to resolve possible false positive matches and make the watch list matching process more accurate. For passengers who have previously flown on an international flight as part of their travel itinerary, the covered aircraft operator may already have the passport information, if the covered aircraft operator was required to collect passport information for the previous flight pursuant to requirements under regulations issued by CBP. For such passengers, TSA would require covered aircraft operators to transmit passport information to TSA as part of the initial SFPD transmission.

For passengers who have reserved an international flight, but who have not yet traveled on an international flight as part of their travel itinerary, covered aircraft operators would collect passport information in accordance with CBP regulations and would be required under this proposed rule to transmit such information to TSA as soon as it is available. In cases where passport information is available, the proposed rule would require covered aircraft operators to transmit the passport information to TSA, to allow TSA to verify the information provided at the time of reservation, facilitate identification of individuals who are on the watch list, and further minimize false positive matches.

The proposed rule leaves individuals with the choice to decline to provide date of birth or gender. For the vast majority of individuals, a decision to forgo providing these data elements should have no effect, and will result in less information being held by aircraft operators, reservations agents, and TSA. For a small number of individuals, however, a decision not to provide date of birth and gender will result in an inability to automatically distinguish them from someone on the watch list. These individuals may be inconvenienced by secondary screening that they otherwise might not have undergone or, if they are a possible match to the No-Fly list they may be required to provide more information than they would have provided had they simply initially provided date of birth and gender. Once the individual provides a verifying identity document to the covered aircraft operator, the proposed rule would require the aircraft operator to update the passenger's SFPD with any of the missing and/or incomplete data elements. Mandating collection of all three data elements would reduce possible matches down to the smallest number of individuals. Accordingly, as part of the evaluation of the proposed rule, TSA will consider, and seeks comments on, whether to mandate collection of not just the full name, but also date of birth and gender.

Secure Flight seeks to balance the competing interests of data collection minimization and reduction of false positives by promoting choice by the individual. Requiring additional information, such as country of citizenship or a phone number, would be helpful in further reducing the risk of a false match

and passenger inconvenience, but it is expected that a sufficient reduction of false positives can be achieved using only the data elements proposed in the NPRM.

To prevent personal information beyond what has been noted above from being accessible to TSA, Secure Flight will employ processes to filter out and prevent any additional personal information beyond what is identified above from being received by TSA. As a result, the Secure Flight system will only receive the personally identifiable information that would be required under the NPRM and described in this PIA.

Itinerary information permits TSA to appropriately prioritize Secure Flight processing, communicate with the covered aircraft operator, facilitate an operational response, and more effectively allocate security resources.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

TSA will use information in the Secure Flight system to identify and protect against potential and actual threats to transportation security, and support the Federal government's counterterrorism efforts by assisting in the identification of individuals who warrant further scrutiny prior to boarding an aircraft or entering a sterile area or who warrant denial of boarding or denial of entry to a sterile area on security grounds. The information TSA collects will be used to conduct operational testing of its ability to connect to the aircraft and airport operators, receive passenger and non-traveler information, conduct watch list matching, and transmit boarding pass printing instructions back to the aircraft and airport operators. During operational testing, aircraft operators would continue to match passengers against the watch lists for domestic flights. Aircraft operators would maintain responsibility for denying issuance of boarding passes and for identifying individuals for enhanced screening during operational testing, but TSA may refer matches identified to the aircraft operator for boarding pass issuance denial or enhanced screening if the operator did not otherwise identify that match. Following successful operational testing required under the proposed rule, TSA, through the implementation of Secure Flight, will assume the responsibility for denying issuance of boarding passes and for identifying individuals for enhanced screening.

Although covered aircraft operators would be required to conduct operational testing with TSA after the final rule is effective, covered aircraft operators may voluntarily choose to begin testing with TSA prior to the publication or effective date of the final rule. This voluntary testing may include testing of the Secure Flight automated matching tool using individuals' full name, date of birth, gender, passport information, itinerary information, reservation control number, record sequence number, record type, and passenger update indicator information if currently collected by covered aircraft operators (as noted in 1.1). This testing may occur contemporaneously with individuals' travel or occur shortly thereafter. Further, under voluntary testing covered aircraft operators may request the above mentioned data

elements full name, date of birth, and gender in order to conduct testing contemporaneously with individuals' travel.

SPFD submitted by aircraft operators to TSA will be used by Secure Flight to conduct watch list matching. The watch list matching process includes automated and, where necessary, manual processes. SPFD will be compared to the watch list (and to a list of individuals cleared through the DHS redress process) by an automated watch list matching process. If the automated comparison determines that the individual is not a match to the watch list, TSA will notify the aircraft operator that the individual may proceed through check-in and normal screening. If the automated comparison identifies a match to the Selectee List, TSA will notify the aircraft operator that the individual must undergo enhanced screening.

If the initial automated comparison indicates a reasonably similar or exact match to a name in the watch list, TSA will instruct the aircraft operator that the individual must be inhibited from obtaining a boarding pass or receiving authorization to enter an airport sterile area. The match will then be manually reviewed as necessary by a Secure Flight analyst who will analyze the available identifying information to determine whether the individual appears to be a match to the individual on the watch list. Additional information about the passenger may have to be obtained from the individual at an airline ticket counter prior to check-in to help resolve a possible match.

If a TSA analyst validates a match between an individual and an identity on the watch list, or if TSA cannot resolve a near match, TSA will send the individual's information to the TSC and request confirmation or resolution of the match. If an individual appears to be a match to the watch list, Secure Flight will send an appropriate instruction to the aircraft or airport operator to deny the individual a boarding pass or authorization into the sterile area. Where warranted, any Federal agency or other public, private, or appropriate foreign government entity may be notified to initiate an operational response. The agency or entity will be provided with sufficient information about the passenger and his or her itinerary to facilitate coordination of the operational response. The Federal Security Director, Federal Air Marshals, or other law enforcement personnel responsible for airport security may also be notified to facilitate a timely law enforcement response to the individual identified in the watch list. Further inquiry by law enforcement may, for example, help resolve a situation of mistaken identity or confirm the determination made in the screening process that an individual should be denied boarding or entry to a sterile area.

Passengers will be matched against watch list updates and updates to the list of persons cleared through the DHS redress process for the duration of each passenger's directional travel. Additionally, passengers will be re-matched to the watch list when there are changes to the original SFPD during the 72 hours before flight departure. If an individual's status changes following boarding pass issuance and/or admittance to a sterile area, appropriate Federal, State, local, tribal, territorial, foreign or international entities may be notified to initiate an operational response

TSA will maintain the identifying information and results of the matching analysis in a matching history for individuals who are identified as potential matches by the automated watch list matching process and are either subsequently cleared or confirmed as matches through manual analysis. For individuals that are matches or potential matches to the watch list, Secure Flight analysts can consult the individual's matching history to expedite the clearance or identification of the individual.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The Secure Flight system results will be analyzed for quality assurance purposes to improve the automated system and to better eliminate false positives.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The Secure Flight system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

TSA mitigates the privacy risk of false positive matches to the watch list by supplementing the initial automated comparison with a manual assessment conducted by a Secure Flight analyst, but only if necessary to complete the watch list matching process. Individuals are provided with the opportunity under Secure Flight's redress process and under the Privacy Act of 1974 to access and correct personal information, subject to the Privacy Act exemptions claimed for Secure Flight records and other applicable legal constraints. Secure Flight does not utilize commercial data verify identities, nor does it use algorithms to assign risk scores to individuals.

TSA has developed a comprehensive approach to promoting compliance with the Fair Information Practices codified in the Privacy Act of 1974, the E-Government Act of 2002, DHS and TSA privacy policies, and Office of Management and Budget (OMB) privacy guidance. Comprehensive privacy requirements are being included in the program requirements to allow TSA to identify privacy issues and risks at each phase of the program and implement privacy principles across Secure Flight systems and operations. The Secure Flight program has designated an individual to work closely with the TSA Director of Privacy Policy and Compliance as well as the DHS Chief Privacy Officer to promote compliance with the published documents for the program, including the SORN and this PIA. This individual will also routinely monitor and review the operations that authorized users perform on personal information according to a schedule to be determined and will be responsible for the implementation of the privacy program.

The Secure Flight Program further minimizes potential privacy risks by integrating administrative, technical, and physical security safeguards as outlined in this PIA to place limitations on the collection of personally identifiable information (PII) and to protect information against unauthorized disclosure, use, modification or destruction. Specifically, administrative safeguards will restrict the permissible uses of personal information and implement the controls for adherence to those uses. As part of technical safeguards employed, Secure Flight will employ role-based access controls and audit logging (the chronicling of information accesses and uses of information) as described in Section 8.0 to control and monitor the use of personal information.

Further, all personnel who are authorized to handle personal information for the Secure Flight program are required to complete TSA privacy training when they join the program and on at least an annual basis thereafter. Personal information will only be disclosed to, and used by, authorized individuals who have a need to know the information in order to perform their duties. These safeguards will further minimize the potential privacy risk that personal information may be improperly used.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

TSA will receive SPFD on non-travelers and passengers, beginning approximately 72 hours before the individual is expected to board a plane or be granted access to a sterile area. In the event that the individual is determined not to be a match by the automated matching process, the Secure Flight program expects to keep that individual's information for no more than 7 days after directional travel has been completed or the non-traveling individual has left the sterile area. Directional travel means that each leg of a round trip itinerary would be assessed separately.

If the automated matching tool determines that an individual is a potential match to an individual on the watch list, TSA expects to retain the information concerning that potential match for seven years. If the potential match is confirmed, TSA expects to retain that confirmed match for 99 years. This retention period is consistent with TSC's NARA-approved record retention schedule for TSDB records.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

TSA is currently working with NARA to establish a record retention schedule that will permit TSA to retain and dispose of records in the Secure Flight system in accordance with the above stated retention cycles.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The proposed record retention periods for Secure Flight would retain records for most individuals encountered by Secure Flight for a short period of time. The vast majority of records are expected to be destroyed within seven days of completion of directional travel. Under the proposed retention periods, records for individuals who are not identified as potential matches by the automated matching tool would be retained for seven days after the completion of the individual's directional travel for audit purposes. Records for individuals who are potential matches would be retained for seven years after the completion of the individual's directional travel in order to expedite future screening and to enable TSA to respond to

any possible legal action. These records would also be available if needed as part of the redress process discussed in section 7.0 of this PIA. TSA is proposing to retain records for individuals confirmed as a positive match to an individual on the watch list for 99 years after the completion of the individual's directional travel in order to support law enforcement and intelligence activities. This retention period for confirmed matches is consistent with the TSC's NARA-approved record retention schedule for records of matches to the TSDB. In case of a terrorist event, records concerning the event, which may include passenger information, would be retained in accordance with a separate TSA record retention schedule covering major security incident records. This information would be retained to support the investigation and documentation of a terrorist event.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Secure Flight will share information within DHS with those offices and components that have a need for the information in the performance of their duties under 5 U.S.C. §552a(b)(1). These purposes may include national security, law enforcement, immigration, intelligence, and other DHS mission-related functions and to provide associated testing, training, management reporting, planning and analysis.

TSA may routinely share an individual's personally identifiable information, itinerary information, and/or airport code, as well as watch list matching analysis and results, and redress information with the following TSA offices: Office of Intelligence (OI) if there is a suspected or actual threat to transportation or national security; Office of Transportation Security Redress (OTSR) to respond to redress requests; Federal Security Directors and Federal Air Marshals in order to facilitate an appropriate law enforcement or operational response to an individual that poses or is suspected of posing a threat to transportation security; Office of Civil Rights and Civil Liberties and Privacy Office to respond to inquiries from individuals; Office of Chief Counsel to assist in the reviews of possible threats to transportation or national security and review responses to inquiries from individuals; Legislative Affairs to respond to inquiries made by members of Congress on behalf of their constituents; and with Freedom of Information Act Office to respond to traveler requests for information.

TSA may also routinely share personally identifiable information with U.S. Customs and Border Protection (CBP) to coordinate the watch list matching function.

4.2 How is the information transmitted or disclosed?

Depending on the urgency, information may be transmitted electronically, in person, in paper format, via facsimile, or by telephone, as required by the circumstances necessitating such sharing. In

most cases, the data will be transmitted between Secure Flight and other systems on the secured DHS information technology (IT) network.

4.3 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information is shared internally with those employees and officials, including contractors, who have a need to know such information in the performance of their duties. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information in the automated system, appropriate to its level of sensitivity. These controls are described below in Section 8.0. Recipients will mitigate any privacy risks through data sharing procedures that may include such things as access controls, re-sharing limits, and other physical, technical, and administrative controls.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

TSA will provide covered aircraft operators and airport operators with boarding pass printing instructions. This will authorize them to take one of the following actions: print boarding/access passes to those who are authorized to receive them, identify individuals for enhanced screening, or deny individuals boarding or sterile area access. The proposed rule would prohibit covered aircraft operators from using the boarding pass printing instructions for any other purposes other than security purposes. To avoid implementing redundant messaging systems for communicating with aircraft operators, Secure Flight will leverage the DHS capabilities to support the connectivity and data transport services to/from the covered aircraft operators for Secure Flight.

In the event of potential matches to the watch lists that cannot be cleared through a manual review process by a Secure Flight analyst, TSA expects to routinely share an individual's personally identifiable information, watch list matching results and analysis, and, if applicable, redress information with the TSC to adjudicate.

TSA also expects to share an individual's personally identifiable information, itinerary, information, and watch list matching analysis and results with law enforcement personnel responsible for airport security who may be notified to facilitate a timely law enforcement response to an individual identified as a potential match the watch list. Further inquiry by law enforcement may also help resolve a

situation of mistaken identity or confirm the determination made in the screening process that an individual should be denied boarding or entry to a sterile area.

Consistent with the routine uses outlined in the Secure Flight Privacy Act System of Records Notice, TSA may share an individual's personally identifiable information, itinerary information, and/or airport code, as well as watch list matching analysis and results, redress information and any of the other information contained in the Secure Flight system with other Federal, state, local, tribal, foreign or international government agencies and organizations for national security, law enforcement, immigration, or intelligence purposes in cases of actual or potential threats to transportation or national security and as necessary to facilitate an operational response to such threats.[14]

In addition, TSA may also share information for additional purposes under the SORN's applicable routine uses including: (1) sharing with an appropriate Federal, State, local, tribal, territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order regarding a violation or potential violation of civil or criminal law or regulation; (2) sharing with the National Archives and Records Administration for proper handling of government records; (3) sharing with the U.S. Department of Justice or other Federal agency for purposes of conducting litigation or administrative proceedings in which the Federal government or its employees are a party or has an interest; (5) sharing with appropriate agencies, entities and persons to protect the individual who is the subject of the record from the harm of identity theft in the case of a data breach affecting this system; and (6) sharing 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. Sharing this information pursuant to this health routine use will assist those agencies in preventing passengers' exposure to communicable diseases, such as transmissible tuberculosis, during aviation travel. Further, it will help those agencies rapidly notify individuals who may have been exposed to such diseases, and prevent further transmission of such diseases as they may pose a threat to transportation and national security if not addressed in a rapid manner. This health routine use may reduce or eliminate potential duplicative reporting of passenger information to U.S. authorities for this purpose. Streamlining the reporting of passenger information for this purpose reduces the economic burden on aircraft operators and promotes the privacy interest of passengers by minimizing the number of times their information is transmitted to U.S. authorities.

Depending on the recipient and the urgency, information may be transmitted electronically, in person, in paper format, via facsimile, or by telephone, as required by the circumstances necessitating such sharing.

[14] For the types of public and private entities that TSA may notify, see "Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses" in the Federal Register notice entitled "Privacy Act of 1974: System of Records; Secure Flight Records."

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. These uses are compatible with the original collection of information. For the types of public and private entities that TSA may notify, see "Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses" in the Federal Register notice entitled "Privacy Act of 1974: System of Records; Secure Flight Records" and the discussion in Section 5.1 above.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Prior to sharing with aircraft operators, aircraft operators will have TSA-approved AOIPs that specify how information will be shared and reflect the scope of the information sharing. The proposed AOIP must set forth the specific means by which the covered aircraft operator will transmit SFPD to TSA, the timing and frequency of transmission, and any other related matters, in accordance with AOIP guidance issued by TSA. Aircraft operators are prohibited from using boarding pass printing instructions provided by Secure Flight for any purpose other than for security purposes.

To avoid implementing redundant messaging systems for communicating with aircraft operators, Secure Flight will leverage the existing DHS system to support the connectivity and data transport services to/from the covered aircraft operators for Secure Flight. Using this secure system, SPFD and boarding pass printing results are transmitted electronically via a network secured using a defense-in-depth strategy and a layered set of security controls to support confidentiality and integrity of data transmission. As necessary, Secure Flight information may be disclosed to authorized parties in person, in paper format, via facsimile, telephonically, or electronically via a secure data network depending on the recipient and the urgency of the request or disclosure.

TSA will transmit to TSC any potential match information, the results of watch list matching, and any analysis conducted in the form of a Referred for Action (RFA) message, which is an automated message between the two agencies. RFAs will be transmitted electronically via the secure DHS network.

External information technology (IT) connections from TSA to any external organizations must be documented and approved with each party's signature in an interagency security agreement (ISA) that outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which DHS shares information must agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the shared information. Any Federal agency receiving this information is required to handle it in accordance with the requirements of the Privacy Act, their applicable SORNs and the Federal Information Management Security Act (FISMA).

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

In general, external sharing will be conducted in accordance with the applicable routine uses under the governing SORN as required by the Privacy Act. Information is shared with external organizations for national security, law enforcement, immigration, or intelligence purposes and as necessary to facilitate an operational response to threats to transportation or national security. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information as appropriate. Any Federal agency receiving information is required to handle it in accordance with the requirements of the Privacy Act, their applicable SORNs and FISMA.

Furthermore, TSA will only share boarding pass printing instructions with covered aircraft operators for purposes of issuing boarding passes to those who are authorized to receive them, identify individuals for enhanced screening, or deny individuals boarding or sterile area access. TSA is proposing to limit the use of boarding pass printing instructions that TSA provides to covered aircraft operators and airport operators for any other purpose other than security purposes.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

TSA will provide notice to individuals through a layered approach. TSA will provide notice through its website (www.tsa.gov) and as a result of the publication of the rulemaking, this PIA and a Privacy Act SORN for the Secure Flight system. In addition to this PIA, TSA is publishing a SORN and NPRM detailing the uses of information in Secure Flight.

Under the proposed rule, prior to collecting information from an individual through a website or an airport kiosk with the capability of accepting a reservation, a covered aircraft operator would be required to make available the following privacy notice prior to collecting information:

"The Transportation Security Administration requires us to collect information from you for purposes of watch list matching, under the authority of 49 U.S.C. section 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. Providing this information is voluntary; however, if it is not provided, you may be subject to additional screening or denied transport or authorization to enter a sterile area. TSA may share information you provide with law enforcement or intelligence agencies or others under its published system of records notice. For more on TSA Privacy policies or to view the system of records notice and the privacy impact assessment, please see TSA's web site at www.tsa.gov."

Covered aircraft operators are also responsible for ensuring that third parties that collect reservation information on their behalf through a website or airport kiosk make available the complete privacy notice.

In the Notice of Proposed Rulemaking for the Secure Flight Program, DHS requests comments on the notice provision generally. In particular, DHS requests comments on how a privacy notice could be provided (if necessary and considering such issues as feasibility, costs, and the effectiveness of the notice) during the collection of information through means not identified in proposed sec. 1560.103.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes, however if the individual declines to provide the requested information, he or she may be subject to additional screening or denied boarding or authorization to enter a sterile area. Individuals who decline to provide their full name will be denied a reservation and will be denied boarding or access to a sterile area.

A covered aircraft operator may, in the ordinary course of business and as part of its reservation process, input data that TSA requires covered aircraft operators to request from individuals, but that the individual did not provide at the time of reservation, such as data from a passenger profile stored by the aircraft operator. In these situations the aircraft operator would be required to include that data as part of the SFPD transmitted to TSA, without obtaining additional consent from the individual, to assist with effective automated watch list matching. Any data elements beyond those required by TSA would be automatically filtered out prior to receipt by the Secure Flight system.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to consent to particular uses of the information collected for the Secure Flight program. However, uses of the information collected through the Secure Flight program are detailed in this PIA, SORN, and NPRM.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The Secure Flight program provides to individuals at or before the time of collection a sufficient number of notice opportunities to reduce the potential risk that those individuals may not be forewarned of the collection and uses of personal information by TSA and of the consequences of not providing the requested information. Notice is provided in a variety of the electronic means utilized by most passengers making reservations. Notice will not be provided in ticket jackets or on airport signage because, as a practical matter, such notice would come too late in the process to provide meaningful opportunity for informed consent.

Individuals participating in the redress process will be provided notice in order to permit them to exercise informed consent prior to providing any information.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Pursuant to a Privacy Act request, individuals may have access to information that they have provided to airline operators that is maintained in the Secure Flight system. Secure Flight will not make available information on the individual, such as watch list matching results or analyses that were not supplied by that individual. Privacy Act requests for access to an individual's record must be in writing and should be addressed to the TSA FOIA Office, Transportation Security Administration (TSA), TSA-20, 601 South 12th Street, Arlington, VA, 22202. Requests should conform to the requirements of 6 CFR part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked
"Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions. An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Alternatively, TSA has established a redress process to assist those individuals seeking to ensure that Secure Flight has access to the most accurate information on the individual for the purposes of determining an individual's match to a name on the watch list. An individual who believes they have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at an airport as a result of the Secure Flight program may initiate the Secure Flight redress process by completing and submitting a Traveler Inquiry Form (TIF) to the DHS Traveler Redress Inquiry Program (TRIP).

Based on the information provided by the individual seeking redress, DHS TRIP will coordinate with TSA to address the request. The DHS TRIP PIA and the TSA Office of Transportation Security Redress (OTSR) PIA are available at www.dhs.gov. Redress requests should be addressed to: Program Manager, DHS TRIP, U.S. Department of Homeland Security, Washington, DC 20528. Additionally, requests for access to the information submitted during the redress process may be made by submitting a request to the DHS TRIP email link TRIP@dhs.gov posted on the DHS TRIP website www.dhs.gov/trip.

7.2 What are the procedures for correcting erroneous information?

The Secure Flight redress process begins when an individual who believes he or she has been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of the Secure Flight program, applies for redress by completing and submitting a TIF to DHS TRIP.

The individual may obtain the forms and information necessary to initiate the redress process on the DHS TRIP web site at www.dhs.gov/trip or by contacting the DHS TRIP office by mail. Written requests may be sent to the DHS TRIP office, and must include the individual's name and current address. DHS will provide the necessary documents and information to individuals through its website or by mail.

The individual must send to the DHS TRIP office the personal information and copies of the specified identification documents. If TSA needs additional information in order to continue the redress process, TSA will so notify the individual in writing and request that additional information. An individual's redress application will be suspended if documentation is not received on or before the established deadlines.

TSA, in coordination with the TSC and other appropriate Federal law enforcement or intelligence agencies, if necessary, will review all the documentation and information requested from the individual, correct any erroneous information, and provide the individual with a timely written response.

TSA's Office of Transportation Security Redress will provide Secure Flight with a Known Misidentified Persons List for use during the watch list matching processes. Updates to this list will be submitted to Secure Flight on a regular basis, and will be incorporated into the watch list matching process.

7.3 How are individuals notified of the procedures for correcting their information?

The redress process for Secure Flight is explained in the NPRM. In addition, individuals are notified of the redress procedures through this PIA, and by both the TSA and DHS websites. TSA and DHS press releases and education campaigns will also provide information on the redress procedures, as well as posters and pamphlets available to passengers at transportation facilities.

7.4 If no formal redress is provided, what alternatives are available to the individual?

An individual who is dissatisfied with the results of DHS TRIP may have the opportunity to submit supplementary information based upon the redress procedures, to TSA. Additionally, upon closing the matter, an individual will be notified in a disposition letter sent by TSA whether he or she may request to have the resolution reconsidered.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

DHS TRIP provides a redress process that furthers the privacy interest of the individual by providing an easy-to-use website that facilitates the submission and processing of redress requests. Because DHS TRIP collects PII directly from the individual, the risk of collecting inaccurate information should be minimized. A PIA for DHS TRIP was published by DHS on January 18, 2007. It is available at the DHS website (www.DHS.gov). In addition, individuals may request access to or correction of their PII pursuant to the Privacy Act.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

User groups that may be granted access to the Secure Flight system will be limited to system administrators, security administrators, IT specialists, and analysts with a need for the information to perform their duties. The system has in place controls to limit access based on user roles and responsibilities, need to know, least privilege, and separation of duties. Rules governing a user's access to the system are applied by the system automatically based on their assigned role. These roles will be approved by the Information Systems Security Officer (ISSO) and any changes in role will need further approval prior to implementation.

Logical access controls restrict users of TSA Secure Flight data. These controls are guided by the principles of least privilege and need to know. User accounts are created with specific job functions in mind and accounts are only granted the necessary access to perform their role as approved by the ISSO. Any changes to user roles require approval of the ISSO. Event logs record system access.

Only TSA Secure Flight personnel and authorized personnel who have passed a background check and completed mandatory privacy and security training will be granted system access.

The Secure Flight system is secured against unauthorized access using a layered defense-in-depth security approach involving procedural and informational safeguards.

Government employees or contractors are assigned roles for accessing the system based on their function. The system administrator grants access to authorized users based on the principles of need to know, least privilege, and separation of duties. The ISSO confirms compliance to policy and manages the activation or deactivation of accounts and privileges as required or when expired. The Secure Flight program will permit personnel that have completed security and privacy training commensurate with their role to access the system.

8.2 Will Department contractors have access to the system?

Contractors supporting TSA's Secure Flight program will have access to the system to perform their official duties including system administration, monitoring, and security functions. Access will be automatically restricted by systems and policies with oversight conducted by Security Officers and management level government personnel. No access will be allowed prior to receiving the necessary clearances and training as required by DHS, TSA and Secure Flight program policy.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Secure Flight personnel, including government personnel and contractors, are required to attend privacy training offered by TSA and role-specific training provided by Secure Flight. This will allow individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties. All DHS personnel, including government personnel and contractors, are required to take privacy training when they begin their employment or contract with DHS.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Secure Flight system has yet to be certified as FISMA compliant. The system received an interim authority to operate in advance of initiation of the testing phase and will receive complete certification and accredited prior to attaining full operational status.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The Secure Flight system maintains an auditing function that tracks all user activities in relation to data including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and other security methods, TSA will prevent unauthorized access to data stored in its system. These controls will meet Federally mandated information assurance and privacy requirements. Both the ISSO and Privacy Officer will periodically review audit logs to confirm compliance with applicable regulations.

The Secure Flight program also embedded security and privacy subject matter experts within core components of the development teams. These individuals help identify potential security and privacy issues to mitigate risk early in the Secure Flight system development.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Identifiable privacy risks of the Secure Flight system include unauthorized access to data, accidental disclosure of PII, and improper modification of data. These risks have been mitigated by defense-in-depth strategy, access controls, auditing, and appropriate oversight. Moreover, the vast majority of individual information is retained for only a short time, thereby reducing risk.

The Secure Flight system is designed to limit the use of PII only to approved uses by authorized parties and protect against inadvertent and unnecessary disclosure. Access to the system and data will be strictly controlled. Only individuals with proper authorization, credentials, training and need to know will be granted access to the system in performance of their duties as approved by the ISSO. Access and audit log reviews, along with other security precautions are in place to further secure system and data access. Processes and policies are in place to further provide that the system use is limited to its intended design while limiting as much as possible the use of PII.

The Secure Flight program embedded security and privacy subject matter experts within core components of the development teams. These individuals have been privy to all levels of decision making, program management, system design and engineering to help identify potential security and privacy issues to mitigate risk early in system's development.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

Secure Flight is a level 1 technology insertion project that establishes passenger watch list matching capabilities within TSA on behalf of DHS. The system is composed primarily of commercial off-the-shelf (COTS) and government off-the shelf products with some customized solutions included. System components include COTS hardware and operating systems along with custom applications running on said systems.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Secure Flight development model is based on the approved TSA System Development Lifecycle (SDLC). The system has been assessed by the DHS investment review process including Enterprise Architecture Center of Excellence I (EACOE) and Integrated Project Review Team (IPRT) and has been approved to initiate activities for the acquisition and design phases.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The primary technologies employed by Secure Flight consist of standard electronic communications and data storage systems. The matching algorithm used to determine if an individual is a potential match to the watch list does not present specific privacy concerns and is deployed in an environment subject to strict administrative, technical and policy controls.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security