DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2007–28972]

RIN 1652–ZA14

Privacy Act of 1974: System of Records; Secure Flight Records

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice to alter an existing system of records.

SUMMARY: The Transportation Security Administration (TSA) is altering and re-publishing the complete system of records, DHS/TSA 019, under the Privacy Act of 1974, known as ''Secure Flight Records,'' for a passenger screening program known as Secure Flight. TSA originally established this system of records and published the system of records notice (SORN) in the **Federal Register** on August 23, 2007 (Part III, 72 FR 48392). TSA received and considered public comments on the SORN and is altering the system of records to reflect the deletion of an exemption previously claimed under 5 U.S.C. 552a(k)(1).

The Secure Flight program implements a mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) 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. Further, section 4012(a)(2) of IRTPA similarly requires the 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. The SORN is being altered to reflect TSA's determination that the system will not contain classified material, and TSA will not claim an exemption under 5 U.S.C. 552a(k)(1).

DATES: Effective upon publication.

FOR FURTHER INFORMATION CONTACT: Peter Pietra, Director, Privacy Policy and Compliance, TSA–36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202–4220; e-mail: *TSAPrivacy@dhs.gov*; or Hugo Teufel III, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528; e-mail: *pia@dhs.gov*.

SUPPLEMENTARY INFORMATION: TSA previously established and published the SORN for this system of records in the **Federal Register** on August 23, 2007 (Part III, 72 FR 48392), and has received and considered public comments. TSA is modifying the ''Exemptions claimed for the system'' section of ''Secure Flight Records'' (DHS/TSA 019) system of records, to reflect the agency's determination that the system will not contain classified material, and TSA will not claim an exemption under 5 U.S.C. 552a(k)(1). TSA will continue to claim exemptions for this system of records pursuant to (j)(2) and (k)(2).

Availability of Notice

You can get an electronic copy using the Internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) Web page at *http://www.regulations.gov*;

(2) Accessing the Government Printing Office's Web page at *http://www.gpoaccess.gov/fr/index.html*; or

(3) Visiting TSA's Security Regulations Web page at *http://www.tsa.gov* and accessing the link for ''Research Center'' at the top of the page.

In addition, copies are available by writing or e-mailing the TSA Privacy Office in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this document.

Background

The Privacy Act of 1974 embodies fair information principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate personally identifiable information contained in a system of records. The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses of the information contained in each system in order to make agency record-keeping practices transparent, to notify individuals regarding the uses to which individually identifiable information is put, and to assist the individual to more easily find such files within the agency. This **Federal Register** notice alters and re-publishes the complete system of records known as ''Secure Flight Records'' (DHS/TSA 019) in support of the Secure Flight program.

The Secure Flight program is based on a mandate from Congress under sections 4012(a)(1) and (2) of IRTPA (Pub. L. 108–458, 118 Stat. 3638, Dec. 17, 2004) that TSA and DHS assume from aircraft operators the comparison of passenger information to the consolidated and integrated terrorist watch list maintained by the Federal Government. In order to carry out this mandate, TSA intends to begin implementation of the Secure Flight program. TSA also published a Notice of Proposed Rulemaking (NPRM) in the **Federal Register** on August 23, 2007 (Part III, 72 FR 48356), that would require certain U.S. aircraft operators and foreign air carriers to provide passenger information to TSA for the purpose of passenger watch list matching against the No Fly and Selectee list components of the consolidated and integrated terrorist watch list, known as the Terrorist Screening Database (TSDB), maintained by the Terrorist Screening Center (TSC).[1] Further, as recommended by the 9/11 Commission, TSA may access the ''larger set of watch lists maintained by the Federal Government.'' [2] Therefore, where warranted by security considerations, TSA may use the full TSDB or other government databases, such as intelligence or law enforcement databases (referred to as ''watch list matching''). 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 database.

Although not required, aircraft operators may voluntarily choose to begin operational testing with TSA prior to publication of a final rule. In the event an aircraft operator begins early operational testing with TSA, the records created as part of that testing will be included in this system of records. During early operational testing, covered aircraft operators may provide watch list matching results conducted by the covered aircraft operators for both domestic and international flights and the passenger

[1] The TSC was 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 Federal Bureau of Investigation (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.

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

data elements outlined in the Secure Flight NPRM.

DHS/TSA 019 will cover certain records TSA creates or receives in the course of operational testing and implementation of the Secure Flight program. Using commercial airline passenger information collected from aircraft operators and foreign air carriers under Secure Flight, TSA, in coordination with the TSC, will compare commercial airline passenger information described below to information about individuals on the No Fly and Selectee list components of the TSDB. In addition, in this watch list matching process , TSA will refer to information generated as a result of the redress process, including information about confirmed, misidentified persons who may previously have been mistaken for individuals on one of the watch lists. Owners or operators of leased or charter aircraft over 12,500 pounds may be permitted to request that TSA screen their passengers, aircraft operators, and lessor(s) through Secure Flight.

Additionally, TSA will apply this screening process to non-traveling individuals who an aircraft or airport operator seeks to authorize to enter an airport sterile area [3] past a security checkpoint for another purpose approved by TSA, such as to escort a minor or a passenger with disabilities.

Information that is maintained in this System of Records may be shared under certain circumstances to confirm watch list matching determinations. This ordinarily will occur when, in an effort to validate a potential match, the Secure Flight program may exchange information with another Federal, state, or local governmental entity, such as Federal, State, or local law enforcement, involved in an operational or informational process associated with watch list matching. Likewise, information may be shared with other Federal agencies where those agencies have information that can be used to distinguish the identity of the individual from that of another individual included on a watch list.

Additionally, certain information may be shared with non-governmental entities where necessary for the sole purpose of effectuating a watch list match determination and the issuance of a boarding pass or gate pass printing instruction to aircraft and/or airport operators.

Other types of information sharing that may result from the routine uses discussed below in this notice include: (1) Disclosure to contractors, grantees, or other individuals who are not DHS employees but have an agency relationship with DHS to accomplish DHS responsibilities; (2) sharing with other Federal, State, local, tribal, foreign or international government agencies and organizations for national security, law enforcement, immigration, or intelligence purposes in response to potential or actual threats to transportation or national security and as necessary to facilitate an operational response to such threats; (3) sharing with Federal, State, local, tribal, foreign or international government agencies and organizations 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; (4) sharing with the National Archives and Records Administration for proper handling of government records; (5) 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; (6) sharing with appropriate agencies, entities and persons to protect an 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 (7) sharing with other governmental agencies or multi-lateral governmental organizations, such as the World Health Organization, to help those agencies prevent exposure to a communicable or quarantinable disease or other significant health threat, such as transmissible tuberculosis, during aviation travel and prevent further transmission of such diseases as these diseases may pose a threat to transportation and national security if not addressed in a rapid manner. Sharing this information pursuant to this health routine use will assist those agencies in preventing passengers' exposure to communicable diseases during aviation travel and it will help those agencies rapidly notify individuals who may have been exposed to such diseases. This health routine use may reduce or eliminate potential duplicative reporting of passenger information to U.S. authorities for this purpose, thereby reducing the number of times this information must be transmitted to proper authorities.

In the course of carrying out the Secure Flight program, TSA will review information from Federal Bureau of Investigation (FBI) systems of records and from systems of records of other law enforcement and intelligence agencies if necessary to resolve an apparent match to the consolidated and integrated terrorist watch list. These may include classified and unclassified governmental terrorist, law enforcement, and intelligence databases, including databases maintained by the Department of Homeland Security, Department of Defense, National Counterterrorism Center, and FBI. Records from these systems are exempt from certain provisions of the Privacy Act because they contain law enforcement investigative information and intelligence information. To the extent records in the Secure Flight Records system are provided by or obtained from such other exempt systems of records, TSA would rely on the Privacy Act exemptions claimed for those systems. Such records or information may be exempt because they include law enforcement or national security investigation records, intelligence-related records, law enforcement encounter records, or terrorist screening records. These could come from various DHS systems, such as the Treasury Enforcement Communications System (TECS) or from other agency systems. After conferring with the appropriate component or agency, TSA may waive applicable exemptions in appropriate circumstances and where it would not interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

SYSTEM OF RECORDS DHS/TSA 019

SYSTEM NAME:

Secure Flight Records.

SECURITY CLASSIFICATION:

Unclassified; Sensitive Security Information.

SYSTEM LOCATION:

Records are maintained at the Transportation Security Administration, 601 South 12th Street, Arlington, VA, and at other secure TSA facilities in Annapolis Junction, Maryland and Colorado Springs, Colorado. Records also may be maintained at the secured facilities of contractors or other parties that perform functions under the Secure Flight program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(a) Individuals who attempt to make reservations for travel on, have traveled on, or have reservations to travel on, a

[3] ''Sterile area'' is defined in 49 CFR 1540.5 and generally means an area of an airport with access limited to persons who have undergone security screening by TSA.

flight operated by a U.S. aircraft operator or a flight into, out of, or overflying the United States that is operated by a foreign air carrier;

(b) Non-traveling individuals who seek to obtain authorization from an aircraft or airport operator to enter the sterile area of an airport;

(c) For flights that TSA grants a request by the operators of leased or charter aircraft over 12,500 pounds to screen the individuals using Secure Flight, the following individuals: (1) individuals who seek to charter or lease an aircraft over 12,500 pounds or who are proposed to be transported on or operate such charter aircraft; and (2) owners and/or operators of such chartered or leased aircraft;

(d) Known or suspected terrorists identified in the TSDB maintained by the TSC; and individuals identified on classified and unclassified governmental databases such as law enforcement, immigration, or intelligence databases; and

(e) Individuals who have been distinguished from individuals on a watch list through a redress process, or other means.

CATEGORIES OF RECORDS IN THE SYSTEM:

(a) Records containing passenger and flight information (e.g., full name, date of birth, gender, redress number, known traveler number, passport information, and itinerary), information about non-traveling individuals seeking access to an airport sterile area in order to escort a minor passenger or for another purpose approved by TSA, and information about passengers on or individuals seeking to charter or lease an aircraft over 12,500 pounds if TSA grants the aircraft owner or operator requests to use Secure Flight.

(b) Records containing information from an individual's form of identification or a physical description of the individual;

(c) Records obtained from the TSC of known or suspected terrorists in the TSDB and records regarding individuals identified on classified and unclassified governmental watch lists;

(d) Records containing the results of comparisons of individuals to the TSDB and watch list matching analyses;

(e) Records related to communications between or among TSA and aircraft operators, airport operators, owners and/or operators of leased or charter aircraft over 12,500 pounds, TSC, law enforcement agencies, intelligence agencies, and agencies responsible for airspace safety or security, regarding the screening status of passengers or non-traveling individuals and any operational responses to individuals identified in the TSDB;

(f) Records of the redress process that include information on known misidentified persons, including any Redress Number assigned to those individuals; and

(g) Records that track the receipt, use, access, or transmission of information as part of the Secure Flight program.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 114, 40113, 44901, 44903, and 44909.

PURPOSE(S):

The Secure Flight Records system will be used 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 seek to enter a sterile area or who warrant denial of boarding or denial of entry to a sterile area on security grounds.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

(1) To the TSC in order to: (a) Determine whether an individual is a positive identity match to an individual identified as a known or suspected terrorist in the watch list; (b) allow redress of passenger complaints; (c) facilitate an operational response, if one is deemed appropriate, for individuals who are a positive identity match to an individual identified as a known or suspected terrorist in the watch list; (d) provide information and analysis about terrorist encounters and known or suspected terrorist associates to appropriate domestic and foreign government agencies and officials for counterterrorism purposes; and (e) perform technical implementation functions necessary for the Secure Flight program.

(2) To contractors, grantees, experts, consultants, or other like persons when necessary to perform a function or service related to the operation, modification, or testing of the Secure Flight program in compliance with the Privacy Act of 1974 as amended.

(3) To aircraft operators, foreign air carriers, airport operators, and the Department of Transportation to communicate passenger watch list matching status and facilitate an operational response, where appropriate, to individuals who pose or are suspected of posing a risk to transportation or national security.

(4) To owners or operators of leased or charter aircraft to communicate passenger screening status and facilitate an operational response, where appropriate, to an individual identified in the watch list.

(5) To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding or to identify individuals who pose or under reasonable suspicion of posing a risk to transportation or national security.

(6) To the Department of Justice or other Federal agency for purposes of conducting litigation or administrative proceedings, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where the Department of Justice (DOJ) or DHS has agreed to represent the employee, or (d) the United States or any agency thereof is a party to the litigation or proceeding or has an interest in such litigation or proceeding.

(7) To the National Archives and Records Administration (NARA) or other Federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

(8) To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual.

(9) To the General Accountability Office, DHS Office of Inspector General or other agency, organization, or individual for the purposes of performing authorized audit or oversight operations but only such information as is necessary and relevant to such audit and oversight functions.

(10) To the 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 when such disclosure is proper and consistent with the performance of the official duties of the person making the disclosure,

(11) To international and foreign governmental authorities in accordance with law and formal or informal international agreements when such disclosure is proper and consistent with the performance of the official duties of the person making the disclosure.

(12) To appropriate agencies, entities, and persons when (a) TSA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) TSA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the

security or integrity of this system or other systems or programs (whether maintained by TSA or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with TSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(13) To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations, including the World Health Organization, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of communicable or quarantinable disease or for combating other significant public health threats; appropriate notice will be provided of any identified health threat or risk. [0]

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Pursuant to routine use twelve (12), TSA may disclose information to a consumer reporting agency in relation to a breach or compromise of information. TSA may need to share information with a credit reporting agency in order to respond to the suspected or confirmed compromise and prevent, minimize, or remedy any resulting harm, such as identity theft. Such sharing would be limited to the purposes outlined in routine use (12).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained at the Transportation Security Administration, 601 South 12th Street, Arlington, VA, and at other secure TSA facilities in Annapolis Junction, Maryland and Colorado Springs, Colorado. Records also may be maintained at the secured facilities of contractors or other parties that perform functions under the Secure Flight program. The records are stored on magnetic disc, tape, digital media, and CD–ROM, and may also be retained in hard copy format in secure file folders or safes.

RETRIEVABILITY:

Data are retrievable by the individual's name or other identifier, as well as non-identifying information such as itinerary.

SAFEGUARDS:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature and provide role-based access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, including encryption, authentication of sending parties, compartmentalizing databases; auditing software and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable TSA and DHS automated systems security and access policies. The system will be in compliance with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance. Access to the computer system containing the records in this system of records is limited to those individuals who require it to perform their official duties. The computer system also maintains a real-time audit of individuals who access the system.

RETENTION AND DISPOSAL:

Records in this system will be retained in accordance with a schedule to be submitted for approval by NARA and other government-wide records schedules, as applicable. TSA is seeking to have records relating to individuals cleared through the automated matching process destroyed within 7 days after completion of the last leg of their directional travel itinerary. The Secure Flight program seeks to retain records reflecting watch list matching analysis and results for individuals who initially appear to be a match for 7 years after the completion of the individual's directional travel itinerary. Records associated with an individual who is determined to be a confirmed match will, consistent with established TSA practice, be retained for 99 years after the date of match confirmation. This retention period is consistent with TSC's NARA-approved record retention schedule for TSDB records.

Records reflecting watch list matching analysis (i.e., match or non-match) for any individual who is confirmed to be a match may also be retained in DHS/TSA 011, Transportation Security Intelligence Service Operations Files (69 FR 71835, Dec. 10, 2004).

Records associated with known misidentified persons, as well as the watch list and other government databases will be retained in accordance with the retention periods for the originating systems.

SYSTEM MANAGER(S) AND ADDRESS:

Donald Hubicki, Director, Secure Flight Program Operations, Transportation Security Administration (TSA), TSA–19, 601 South 12th Street, Arlington, VA 22202.

NOTIFICATION PROCEDURE:

To determine whether this system contains records relating to you, write to the FOIA and Privacy Act Office, Transportation Security Administration (TSA), TSA–20, 601 South 12th Street, Arlington, VA 22202.

RECORDS ACCESS PROCEDURES:

Requests for records access must be in writing and should be addressed to FOIA and Privacy Act 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.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (''TRIP'') (See 72 FR 2294, January 18, 2007). Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can correct erroneous data stored in Secure Flight and other data stored in other DHS databases through one application. Additionally, for further information on the Secure Flight Program and the redress options please see the accompanying Privacy Impact

Assessment for Secure Flight published on the DHS Web site at *http://www.dhs.gov/privacy* in this edition of the **Federal Register** and at DHS.GOV. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), TSA–901, 601 South 12th Street, Arlington, VA 22202–4220, or online at *http://www.dhs.gov/trip.*

CONTESTING RECORDS PROCEDURES:

Same as ''Notification Procedure'' and ''Record Access Procedure'' above.

RECORD SOURCE CATEGORIES:

Information contained in the system is obtained from U.S. aircraft operators, foreign air carriers, the owners and operators of leased or charter aircraft over 12,500 pounds who request TSA screening, the TSC, TSA employees, airport operators, Federal, State, local, international and other governmental law enforcement , intelligence, immigration, and counterterrorism agencies, other Federal agencies responsible for airspace safety or security, and the individuals to whom the records in the system pertain.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

No exemption will be asserted with respect to identifying information or flight information obtained from passengers and aircraft owners or operators.

This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, in accordance with 5 U.S.C. 552a(j)(2) and (k)(2), TSA claims the following exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f); and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information. Certain portions or all of these records may be exempt from disclosure pursuant to these exemptions.

Issued in Arlington, Virginia, on November 2, 2007.

John Kropf,

Deputy Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E7–21908 Filed 11–8–07; 8:45 am]

BILLING CODE 9110–05–P