[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. DHS-2012-0068]

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: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS), Transportation Security Administration (TSA) is altering and republishing an existing system of records notice (SORN) titled Department of Homeland Security /Transportation Security Administration 019 (DHS/TSA-019), Secure Flight Records, for the passenger and non-traveler screening program known as Secure Flight. TSA is republishing this SORN to reflect additions to TSA's screening capabilities designed to better focus enhanced passenger screening efforts on individuals likely to pose a threat to civil aviation, and to facilitate the secure and efficient travel of the vast majority of the traveling public by distinguishing them from individuals on federal government watch lists. This SORN includes modifications in the following areas of the SORN: categories of individuals, categories of records, purpose(s), routine uses, disclosure to consumer reporting agencies, data retention and disposal, notification procedure, records access procedures, and the record source categories.

DATES: Submit comments on modifications to routine use 3 on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

This updated system will be effective upon publication except that the change to routine use 3 will be effective 30 days after date of publication in the Federal Register.

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0068 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Peter Pietra, Director, Privacy Policy and Compliance, TSA-36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598-6036; email: *TSAPrivacy@dhs.gov*; or Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528; email: *privacy@dhs.gov*.

SUPPLEMENTARY INFORMATION:

Availability of Notice

You may obtain 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 notice.

Background

The Transportation Security Administration is responsible for security in all modes of transportation and performs passenger and baggage screening at the Nation's airports. Prior to the implementation of the TSA Secure Flight program, this screening was supplemented by aircraft operators who performed passenger watch list matching against the federal No Fly and Selectee Lists, as required under security directives issued by TSA in 2002. Aircraft operators also conducted this watch list matching process for certain non-traveling individuals[1] authorized to enter the sterile area[2] of an airport.

The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) recommended that watch list matching be performed by TSA using the

[1] "Non-traveling individual" or "non-traveler" means an individual to whom a covered aircraft operator or covered airport seeks to issue an authorization to enter the sterile area of an airport in order to escort a minor or passenger with disabilities or for some other purpose permitted by TSA. The term does not include employees or agents of an airport or aircraft operators or other individuals whose access to a sterile area is governed by another TSA requirement. 49 CFR § 1560.3.

[2] "Sterile area" means a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier through the screening of persons and property. 49 CFR § 1504.5.

"larger set of watch lists maintained by the Federal Government."[3] In response, under section 4012(a)(1)-(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[4] Congress directed TSA and DHS to assume from aircraft operators the function of comparing airline passenger information to data in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC).[5] Consistent with this statutory directive, TSA promulgated the Secure Flight Final Rule[6] for the purpose of enhancing the security of air travel in the United States and to support the federal government's counter-terrorism efforts by assisting in the detection of individuals on federal government watch lists who seek to travel by air, and to facilitate the secure travel of the public. By November 2010, TSA fully assumed the watch list matching function from aircraft operators and air carriers.

TSA established the Secure Flight system of records and published the SORN in the **Federal Register** on August 23, 2007.[7] TSA altered and republished the SORN in the **Federal Register** on November 9, 2007.[8] TSA is amending the Secure Flight SORN again to reflect additions to TSA's screening capabilities as discussed below.

TSA uses Secure Flight to conduct watch list matching against the No Fly and Selectee List components of the TSDB. Where warranted by security considerations, Secure Flight also matches against the full TSDB and other government databases. In

[3] "National Commission on Terrorist Attacks Upon the United States," page 393 (July 22, 2004).
[4] Pub. L. 108-458, 118 Stat. 3638 (December 17, 2004).
[5] 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 to 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.
[6] 73 FR 64018 (Oct. 28, 2008).
[7] 72 FR 48392.
[8] 72 FR 63711.

addition, Secure Flight matches against the list of individuals whom the Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) has identified to DHS as persons who should not be permitted to board an aircraft due to public health concerns.[9]

TSA also uses Secure Flight to match air travelers and other individuals seeking access to airport sterile areas against a list of individuals who have each been assigned a unique redress number by the DHS Traveler Redress Inquiry Program (TRIP).[10] TSA also may collect and use a passenger's "Known Traveler Number" if available. A Known Traveler Number is a unique number assigned to Known Travelers for whom the federal government has conducted a security threat assessment and determined do not pose a security threat.[11] TSA did not use this capability when it initially assumed responsibility for passenger screening using Secure Flight. In October 2011, however, TSA announced the TSA Pre✓™ pilot program.[12] TSA initiated TSA Pre✓™ as a proof of concept at four U.S. airports, starting with individuals enrolled within U.S. Customs and Border Protection (CBP) Trusted Traveler programs[13] and certain airline frequent flyer program members.[14] The purpose of the proof of concept was to evaluate

[9] To accomplish this list matching function, Secure Flight ingests copies of these lists of individuals identified on other government systems to minimize the processing time when Secure Flight receives passenger travel data.
[10] http://www.dhs.gov/files/programs/gc_1169673653081.shtm.
[11] *See* 49 CFR 1560.3.
[12] *See TSA Pre™ Pilot Starts Today at Select Airports to Further Enhance Security*, TSA Office of Public Affairs (October 4, 2011), www.tsa.gov/press/releases/2011/1004.shtm.
[13] CBP Trusted Traveler programs include Global Entry, SENTRI, and NEXUS. *See* www.cbp.gov/xp/cgov/travel/trusted_traveler. For individuals in the CBP Trusted Traveler programs, TSA receives from CBP a list of eligible travelers that is ingested into Secure Flight to minimize the processing time when Secure Flight receives passenger travel data. Eligible members of these programs provide their Known Traveler number to aircraft operators for transmittal to Secure Flight.
[14] For airline frequent flyers, TSA has developed eligibility criteria and partnered with aircraft operators that identify frequent flyers who meet those criteria. Those frequent flyers are given the opportunity to opt into the TSA Pre✓™ program. When those passengers' travel data are submitted by the aircraft operators

capabilities to identify air travelers who are lower risk and eligible for expedited security screening at the airport checkpoints, and to test expedited screening processes. The Known Travelers participating in the proof of concept volunteered information that permitted TSA to make risk assessments *before* the individual arrives at the airport.

Earlier this year, TSA began the transition of the TSA Pre✓™ program—including individuals in CBP Trusted Traveler programs and certain airline frequent flyer program members—from proof of concept to an operational status.[15] TSA is expanding the availability of TSA Pre✓™ to additional U.S. airports and populations, such as eligible members of the U.S. Armed Forces and certain active security clearance holders.[16] By identifying passengers who are low risk and providing them expedited screening, TSA Pre✓™ enables the agency to better focus its screening efforts on individuals who are more likely to pose a threat to civil aviation.

As part of the effort to identify individuals that are low risk, TSA also is creating and maintaining a watch list of individuals who are disqualified from eligibility from TSA Pre✓™, for some period of time or permanently, because they have been involved in violations of security regulations of sufficient severity or frequency. Disqualifying violations of aviation security regulations may involve violations at the airport or on board aircraft, such as a loaded firearm that is discovered in carry-on baggage at the checkpoint, or a threat to use a destructive device against a transportation conveyance,

---

to Secure Flight, the aircraft operator also includes a designator code that identifies the passenger as eligible for expedited screening. See www.tsa.gov/what_we_do/escreening.shtm.

[15] *See TSA Pre✓™ Screening Benefits Expanding to Additional Airports,* TSA Office of Public Affairs (March 30, 2012), www.tsa.gov/press/releases/2012/0330.shtm; DHS/TSA/PIA-018(e) - Secure Flight Program Update, www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf.

[16] As additional populations are added to the TSA Pre✓™ program, additional lists of eligible individuals will be ingested by Secure Flight. The Secure Flight Privacy Impact Assessment (PIA) will be updated to reflect that information. See www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf.

facilities, or personnel. The TSA Pre✓™ Disqualification List will be generated by TSA's Performance and Results Information System (PARIS).[17]

Consistent with its ongoing efforts to focus on passengers who are more likely to pose a threat to civil aviation, and following the failed terrorist attack on an international flight bound for Detroit on December 25, 2009, the Secure Flight program began matching passengers on international flights bound for the United States against a list of individuals requiring enhanced screening that is generated through CBP's Automated Targeting System (ATS).[18] ATS uses threat-based intelligence scenarios designed to identify international travelers who are more likely to pose a threat and for whom enhanced screening is appropriate. TSA receives from CBP a continuously updated list of individuals identified through these scenario rules for use in Secure Flight passenger screening. Oversight is exercised by the DHS Offices of Privacy, Civil Rights and Civil Liberties, and General Counsel to ensure that the threat-based intelligence is appropriately applied. After they arrive in the United States, some of these international travelers also may receive enhanced screening prior to subsequent domestic and international outbound flights for a period of time, again based on threat-based, intelligence-driven scenario rules.

TSA receives from CBP an Electronic System for Travel Authorization (ESTA) status code for international travelers. ESTA is an automated system used by CBP to determine the eligibility of visitors to travel to the United States under the Visa Waiver

[17] PARIS is an enforcement and inspections system for all modes of transportation for which TSA has security related duties, and maintains records related to the investigation or prosecution of violations or potential violations of Federal, State, local, or international criminal law. For additional information, *see* DHS/TSA-001 Transportation Security Administration Transportation Security Enforcement Record System (TSERS), 75 FR 28042 (May 19, 2010).

[18] *See Secretary Napolitano Announces New Measures to Strengthen Aviation Security,* DHS Office of the Press Secretary (April 2, 2010).

Program and whether the traveler poses any law enforcement or security risk. In order to eliminate multiple messages to the airlines from CBP and TSA on a single passenger, Secure Flight transmits the ESTA status code for international travelers to the aircraft operator as part of the boarding pass printing result.

Finally, TSA is adding a clause to subsection (a) of the Category of Individuals to ensure that, when requested by a U.S. government agency or institution, TSA may use Secure Flight to vet passengers on U.S. government operated, chartered, or leased flights. A corresponding change to routine use (3) is being made to permit disclosure of information to the U.S. government agency for screening status or operational response.

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS/TSA is altering and republishing DHS/TSA SORN DHS/TSA-019, titled Secure Flight Records (72 Fed. Reg. 63711, November 9, 2007). Consistent with the discussion above, the following modifications are being made to the DHS/TSA-019 Secure Flight Records system of records:

- The Categories of Individuals section is updated as follows:
    - We have added a category of individuals to subsection (a) to ensure that U.S. government operated flights are covered, including flights leased or chartered by the U.S. government.
    - We have rewritten subsection (c) to clarify that it addresses individuals involved with chartered or leased aircraft "with a maximum take-off weight" over 12,500 pounds; and
    - We have added a new subsection (f) to expressly include individuals who are identified as Known Travelers.

- The Categories of Records section is updated as follows:
    - We have amended subsection (a) to note that TSA receives from aircraft operators the designator code used to verify certain travelers' frequent flyer status.
    - Subsection (a) also was amended to clarify that Secure Flight may receive Secure Flight Passenger Data (SFPD)[19] for individuals who seek to charter, lease, operate, or be transported on aircraft "with a maximum take-off weight" over 12,500 pounds, and owners and/or operators of such aircraft,
    - We have revised subsection (d) to reflect that matching analyses and results may include lists generated by other classified and unclassified government watchlists. As discussed above such lists include CBP ATS, the TSA Pre✓™ Disqualification list, and the CDC Do Not Board list.
    - We have inserted a new subsection (h) to expressly include the Electronic System for Travel Authorization (ESTA) status code for international travelers as a category of records,
    - We have inserted a new subsection (i) to expressly include records about Known Travelers.
- The Purpose(s) section is updated to reflect that, in addition to assisting in the detection of individuals identified on federal government watch lists who seek to

[19] SFPD is the following information regarding a passenger or non-traveling individual: full name, date of birth, gender, redress number or Known Traveler Number, passport information, reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information. 49 CFR § 1560.3.

travel by air, Secure Flight also is used to identify air travelers who are lower risk and eligible for expedited security screening at the airport checkpoints.

- The Routine Uses section is updated as follows:
    - We have rewritten routine use (2) to conform to a standard DHS routine use pertaining to the sharing of information with contractors when necessary.
    - We have amended routine use (3) to more accurately reflect that TSA discloses the passenger screening status, not the watch list matching status, to airlines, airports, and the Department of Transportation, and to reflect that passenger screening information may be disclosed to U.S. government agencies that operate, charter, or lease aircraft. This would permit, for example, the Department of Defense (DoD) to request that passengers on a DoD operated or chartered flight be vetted through Secure Flight.
    - We have amended routine use (4) to make it consistent with routine use (3) providing for disclosure regarding individuals who pose or are suspected of posing a risk to transportation or national security.
    - We have deleted from routine use (9) the reference to the DHS Office of Inspector General since such disclosures would be accomplished pursuant to the Privacy Act under 5 U.S.C. §552a(b)(1) rather than pursuant to a routine use.
- The Disclosure to Consumer Reporting Agencies section is being changed to reflect that disclosures in connection with the Debt Collection Act of 1982 (Pub.

L. 97-365) are not part of this system of records. Routine use 12 remains in place to permit disclosures in the event of a data breach.

- The Retention and Disposal section is amended to reflect that the retention schedule was approved by NARA. This section also was amended to reflect that lists of individuals in Secure Flight, such as Known Traveler lists and the TSA Pre✓™ Disqualification list, will be deleted or destroyed when superseded.
- The System Manager and Notification Procedure section has been updated to reflect updated contact information.
- The Records Access Procedures section has been updated to reflect the correct zip code for the TSA Freedom of Information Act Office.
- The Records Access Procedures section also was revised to clarify that individuals who believe they have been improperly denied entry by CBP may submit a redress request through DHS TRIP.
- The Record Source Categories section is updated to clarify that Secure Flight may receive information from all three branches of the Federal government, as well as from private entities (*e.g.,* airlines) that participate in the Known Traveler program.
- The Exemptions Claimed for the System category is updated to include non-travelers to whom a covered aircraft operator or covered airport seeks to issue an authorization to enter the sterile area of an airport.

Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the federal government agencies collect,

maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

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 that are contained in each system in order to make agency recordkeeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/TSA-019 Secure Flight Records system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

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 (TSA), 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 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, or flights operated by the U.S. government, including flights chartered or leased by the U.S. government;

(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 with a maximum take-off weight over 12,500 pounds to screen the individuals using Secure Flight, the following individuals: (1) individuals who seek to charter or lease an aircraft with a maximum take-off weight 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) (1) Known or suspected terrorists identified in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC); and (2) individuals identified on classified and unclassified governmental databases such as law enforcement, immigration, or intelligence databases;

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

(f) Individuals who are identified as Known Travelers for whom the federal government has conducted a security threat assessment and determined do not pose a security threat.

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, frequent flyer designator code or other identity authentication/verification code obtained from aircraft operators, and itinerary); records containing information about non-traveling individuals seeking access to an airport sterile area for a purpose approved by TSA; and records containing information about individuals who seek to charter, lease, operate or be transported on aircraft with a maximum take-off weight over 12,500 pounds if TSA grants the request of an aircraft owner or operator 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 matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental watch lists;

(e) Records related to communications between or among TSA and aircraft operators, airport operators, owners and/or operators of leased or charter aircraft with a maximum take-off weight 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;

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

(h) Electronic System for Travel Authorization status code generated by U.S. Customs and Border Protection (CBP) for international travelers; and

(i) Records containing information about individuals who are identified as Known Travelers.

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. It also will be used to identify individuals who are lower risk and therefore may be eligible for expedited security screening at the airport checkpoints. Both of these functions are designed to facilitate the secure travel of the public.

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 and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other

assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

(3) To aircraft operators, foreign air carriers, airport operators, the Department of Transportation, and the Department of Defense or other U.S. government agencies or institutions, to communicate individual screening 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 individual screening status and facilitate an operational response, when appropriate, to individuals who pose or are suspected of posing a risk to transportation or national security.

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

(6) To the Department of Justice (DOJ) or other Federal agency for purposes of conducting litigation or administrative proceedings, when: (a) the Department of Homeland Security (DHS), or (b) any employee or former employee of DHS in his/her official capacity, or (c) any employee or former employee of DHS in his/her individual capacity where the 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 in response to an inquiry from that congressional office made at the request of the individual.

(9) To the Government Accountability Office 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, regulation, or order 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.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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. The system has role-based access control to sensitive data, physical access control to DHS facilities, auditing software, and confidentiality of communications, including encryption, authentication of sending parties, compartmentalizing databases. Personnel is conducted 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 and National Institute of Standards and Technology 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 relating to an individual determined by the automated matching process to be neither a match nor or potential match to a watchlist will be destroyed within seven days after completion of the last leg of the individual's directional travel itinerary. Records relating to an individual determined by the automated matching process to be a potential watch list match will be retained for seven years after the completion of the individual's directional travel itinerary. Records relating to an individual determined to be a confirmed watchlist match will be retained for 99 years after the date of match confirmation.

Lists of individuals stored in Secure Flight, such as individuals identified as Known Travelers and individuals who have been disqualified from eligibility to receive expedited screening as a result of their involvement in certain security incidents, will be deleted or destroyed when superseded by an updated list.

SYSTEM MANAGER(S) AND ADDRESS:

Secure Flight Mission Support Branch Manager, Transportation Security Administration, TSA-19, 601 South 12th Street, Arlington, VA, 20598-6019.

NOTIFICATION PROCEDURE:

To determine whether this system contains records relating to you, write to the Freedom of Information Act Office, Transportation Security Administration, TSA–20, 601 South 12th Street, Arlington, VA 20598-6020.

RECORDS ACCESS PROCEDURES:

Requests for records access must be in writing and should be addressed to the Freedom of Information Act Office, Transportation Security Administration, TSA–20, 601 South 12th Street, Arlington, VA, 20598-6020. 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.

Individuals who believe they have been improperly denied entry by CBP, refused boarding for transportation, or identified for additional screening may submit a redress request through the DHS Traveler Redress Program ("TRIP") (see 72 Fed. Reg. 2294, January 18, 2007). 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 website at *www.dhs.gov/privacy*. Redress requests should be sent to: DHS Traveler Redress

Inquiry Program (TRIP), TSA–901, 601 South 12th Street, Arlington, VA 20598-6036 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 with a maximum take-off weight over 12,500 pounds who request TSA screening, the TSC, TSA employees, airport operators, Federal executive branch agencies, Federal judicial and legislative branch entities, State, local, international, and other governmental agencies, private entities for Known Traveler program participants, 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, non-travelers, and aircraft owners or operators.

This system, however, may contain records or information recompiled from or created from information contained in other systems of recordsthat 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.

November 6, 2012

_____

Jonathan R. Cantor

Chief Privacy Officer, Acting

Department of Homeland Security

[FR Doc. 2012-28058 Filed 11/16/2012 at 8:45 am; Publication Date: 11/19/2012]