DEPARTMENT OF HOMELAND SECURITY
Office of the Secretary
[Docket No. DHS–2013–0020]


AGENCY: Department of Homeland Security.

ACTION: Notice of modified Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, “Department of Homeland Security/Transportation Security Administration—DHS/TSA–019 Secure Flight Records System of Records.” This system of records allows the Department of Homeland Security/Transportation Security Administration to collect and maintain records on aviation passengers and certain non-travelers to screen such individuals, before they access airport sterile areas or board aircraft, in order to identify and prevent a threat to aviation security or the lives of passengers and others. TSA is reissuing this system of records to update the categories of records to include whether a passenger will receive expedited, standard, or enhanced screening. The primary impact of this change will be the identification of additional passengers who are eligible for expedited screening at participating airport security checkpoints. This updated system will be included in the Department of Homeland Security’s inventory of system of records.

DATES: Submit comments on or before October 10, 2013. This updated system will be effective upon publication except that the change to the categories of records will be effective 30 days after date of publication in the Federal Register.

ADDRESSES: You may submit comments, identified by docket number DHS–2013–0020 by one of the following methods:

- Fax: 202–343–4010.

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.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Peter Pietra, Privacy Officer, TSA–36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20508–6036; email: TSPAprivacy@dhs.gov. For privacy questions, please contact: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS)/Transportation Security Administration (TSA) proposes to update and reissue a current DHS system of records titled, “DHS/TSA–019 Secure Flight Records System of Records.” This system of records notice was last updated on November 19, 2012. TSA is modifying the DHS/TSA–019 Secure Flight Records System of records Categories of Records section in subsection (a) to add records containing the results from TSA’s intelligence-driven risk-based analysis of Secure Flight Passenger Data (SFPD). Secure Flight Passenger Data is full name, gender, date of birth, redress number or Known Traveler number, passport information (if applicable), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information. 49 CFR § 1560.

Sec. 4012(a)(1)–(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress directed TSA and DHS to assume from aircraft operators the function of comparing aircraft operator passenger information to data in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC).

1 77 FR 60949 (Nov. 19, 2012).
3 The TSC maintains the Federal government’s consolidated and integrated terrorist watch list, known as the TSDB. The TSDB 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...
In order to implement this statutory directive, TSA promulgated the Secure Flight Program regulations \(^4\) 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. TSA fully assumed the watch list matching function from aircraft operators and air carriers by November 2010.

TSA established the Secure Flight system of records and published the System of Records Notice (SORN) in the Federal Register on August 23, 2007.\(^5\) TSA updated and republished the SORN in the Federal Register on November 9, 2007,\(^6\) and again on November 19, 2012.\(^7\) Information collection falls under OMB Control Number 1652–0046.

As part of TSA’s ongoing efforts to identify appropriate security screening for commercial aviation travelers, TSA plans to implement a risk-based analysis of passenger and flight data provided through the computer system that processes Secure Flight and other data. TSA is amending the Secure Flight SORN to reflect this addition to TSA’s passenger prescreening capabilities. Prescreening involves the use of information to make decisions before the passenger receives a boarding pass, to determine what level of physical screening the passenger will receive when he or she arrives at the TSA airport security checkpoint. This change is part of TSA’s ongoing efforts to identify appropriate screening for travelers, including those who present a lower security risk. The primary result of this change will be the identification of passengers who are eligible for expedited screening at participating airport security checkpoints.\(^8\)

### II. 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 where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

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

DEPARTMENT OF HOMELAND SECURITY (DHS)/TRANSPORTATION SECURITY ADMINISTRATION (TSA)-019.

**SYSTEM NAME:**


**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.

---

\(^{10}\) Nationwide: Expedited Screening Begins at Raleigh-Durham International Airport, http://www.tsa.gov/press/releases/2013/03/26/secure-flight-begins-at-raleigh-durham-international-airport

\(^{11}\) 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 § 1540.5.
CATHERINES OF INDIVIDUALS COVERED BY THE
SYSTEM:

(a) Individuals who attempt to make
reservations for flight 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
airport 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.

CATHERINES OF RECORDS MAINTAINED 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 the results
of risk-based analysis in the TSA
passenger prescreening system,
including boarding pass printing results;
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 charter an 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
distinguished 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;

(b) 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
screening at the airport security
checkpoint. 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
THE 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, cooperation
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 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.

To aircraft operators or foreign air
carriers, to communicate individual
screening status, where appropriate, to
individuals who are a low 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, where
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, or foreign,
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 agencies, grants, or
agreements, agreements, or other
assignments for DHS, where
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.

To aircraft operators or foreign air
 carriers, to communicate individual
screening status, where appropriate, to
individuals who are a low risk to
transportation or National security

(7) To officials, persons, or
organizations subject to the same
Privacy Act requirements and
limitations on disclosure as are
applicable to DHS officers and employees.
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 2006.

(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, or foreign 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, remedy, or address such harm.

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 disk, 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 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 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 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 AND ADDRESS:


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.

RECORD 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 FR 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 Web site 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 RECORD 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 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. A Final Rule was promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and can be found at 72 FR 63706 (Nov. 9, 2007).


Jonathan R. Cantor,

[FR Doc. 2013–21980 Filed 9–9–13; 8:45 am]

BILLING CODE 9110–06–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2013–0040]

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA–021 TSA Pre✓™ Application Program System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, “Department of Homeland Security/Transportation Security Administration—DHS/TSA–021 TSA Pre✓™ Application Program System of Records.” This system of records allows the Department of Homeland Security/Transportation Security Administration to collect and maintain records on individuals who voluntarily submit information to the Transportation Security Administration for use by the agency to perform a security threat assessment. The security threat assessment will be used to identify persons who pose a low risk to transportation security and therefore may be eligible for expedited screening at participating U.S. airport security checkpoints. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking elsewhere in the Federal Register to exempt some records from this system of records from certain provisions of the Privacy Act. This newly established system will be included in the Department of Homeland Security’s inventory of systems of records.

DATES: Submit comments on or before October 10, 2013. This new system will be effective October 10, 2013.

ADDRESSES: You may submit comments, identified by docket number DHS–2013–0040 by one of the following methods:

• Fax: 202–343–4010.
• Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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: For general questions, please contact: Peter Pietra, TSA Privacy Officer, TSA–036, 601 South 12th Street, Arlington, VA 20598–6036; or email at TSPAprivacy@dhs.gov. For privacy questions, please contact: Jonathan R. Cantor, (202) 343–1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS)/Transportation Security Administration (TSA) proposes to establish a new DHS system of records titled, “DHS/TSA–021 TSA Pre✓™ Application Program System of Records.” TSA is establishing this new system of records to inform the public of the collection, maintenance, dissemination, and use of records on individuals who voluntarily submit personally identifiable information to the TSA Pre✓™ Application Program. TSA will use the information provided by applicants 1 to the Program to perform a

---

1 Further information on information collection can be found in Intent To Request Approval From OMB of One New Public Collection of Information: TSA Pre✓™ Trusted Traveler Program; Republication, 78 FR 45256 (July 26, 2013) (republished for technical correction).