9110-05-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0076]

Privacy Act of 1974; Department of Homeland Security Transportation Security Administration - DHS/TSA-019 Secure Flight Records System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice 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 to the lives of passengers and others. TSA is reissuing this system of records to update the categories of records to include records containing risk-based assessments generated by aircraft operators using data in their Computer-Assisted Passenger Prescreening Systems (CAPPS). These CAPPS assessments are used in risk-based analysis of Secure Flight and other prescreening data that produces a boarding pass printing result for each passenger. This change identifies additional passengers who may be eligible for expedited screening at airport security checkpoints. This updated system will continue to

be included in the Department of Homeland Security's inventory of record systems. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DATES: Submit comments 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 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-2014-0076 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: Karen L. Neuman, 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: For general questions, please contact: Peter Pietra, Privacy Officer, TSA-36, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598-6036; email: TSAPrivacy@dhs.gov. For

privacy questions, please contact: Karen L. Neuman, 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 September 10, 2013.[1]

TSA is modifying DHS/TSA-019 by adding Computer-Assisted Passenger Prescreening System (CAPPS) assessments received from aircraft operators to the Categories of Records. CAPPS assessments are the product of a risk analysis of passenger name records (PNR)[2] and other information associated with flight reservations that aircraft operators collect in the ordinary course of business. These PNRs and other data provide risk indications and are used to assess passenger risk on a per flight basis. The CAPPS assessment, in turn, is used in the risk-based analysis of Secure Flight Passenger Data (SFPD)[3] and other prescreening data that produce a boarding pass printing result for each passenger. The early use of CAPPS by aircraft operators was to

[1] 78 FR 55270 (Sept. 10, 2013).

[2] A PNR contains details about an individual's travel on a particular flight, including information provided by the individual when making the flight reservation. Though the content of PNRs varies among airlines, PNRs may include: (1) passenger name; (2) reservation date; (3) travel agency or agent; (4) travel itinerary information; (5) form of payment; (6) flight number; and (7) seating location. *See* DHS/TSA–017 Secure Flight Test Records, 70 FR 36320 (June 22, 2005). Some PNR data collected by aircraft operators provide evidence of potential security risks, and other data provide indications of low security risk. Other PNR data are security neutral.

[3] SFPD 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 C.F.R. 1560.

identify passengers other than those on watch lists who merited additional screening. TSA now will incorporate the CAPPS assessment to identify low-risk passengers who may be eligible for expedited screening in airports with TSA Pre✓® lanes. By receiving a CAPPS assessment (as opposed to the underlying data used to arrive at that assessment), TSA obtains important security value from information without receiving all the underlying data that are generated when individuals make their flight reservations.

TSA established the Secure Flight system of records and published the System of Records Notice (SORN) in the Federal Register on August 23, 2007.[4] TSA updated and republished the SORN in the Federal Register on November 9, 2007,[5] on November 19, 2012,[6] and on September 10, 2013.

Background on CAPPS

In response to the changing threat of terrorism,[7] President Clinton established the White House Commission on Aviation Safety and Security (Commission) in 1996.[8] In its final report,[9] the Commission recognized that aviation security is a national security issue and recommended that the Federal Aviation Administration (FAA) "work with airlines and airport consortia to ensure that all passengers are positively identified and subjected to security procedures before they board aircraft."[10] Specifically, the Commission recommended that the FAA, "based on information already in [air carriers']

[4] 72 FR 48392.
[5] 72 FR 63711.
[6] 77 FR 69491.
[7] In addition to overseas threats from foreign terrorists, people and places in the United States were becoming targets, and Americans joined the ranks of terrorists. The 1993 and 1995 bombings of the World Trade Center in New York, and the Federal Building in Oklahoma City, respectively, were clear examples of the shift, as was the 1996 conviction of Ramzi Yousef for attempting to bomb American airliners over the Pacific Ocean.
[8] Executive Order 13015, *White House Commission on Aviation Safety and Security*,61 FR 43937 (Aug. 22, 1996).
[9] White House Commission on Aviation Safety and Security, Final Report to President Clinton, February 12, 1997, found at www.fas.org/irp/threat/212fin~1.html (hereinafter *Report*).
[10] *Id.* at section 3.7.

computer databases," leverage that industry investment by separating passengers "into a very large majority who present little or no risk, and a small minority who merit additional attention."[11] The Commission supported the development and implementation of automated passenger screening systems such as the system then under development by the FAA and Northwest Airlines.

Following the Commission's report, CAPPS was created by the FAA[12] to serve as a feasible alternative to conducting the Commission-recommended 100 percent checked baggage matching and explosive detection screening.[13] CAPPS was designed "to exclude from the additional security measures the great majority of passengers who are very unlikely to present any threat and, conversely, to identify passengers to whom heightened security measures should be applied."[14] The FAA evaluated whether PNR and other data associated with flight reservations that the aircraft operator collected in the ordinary course of business provided indicators of high security risk or low risk, or whether the data were risk neutral.[15] Aircraft operators ran CAPPS in their reservation systems for originating passengers who checked bags prior to passenger boarding using the FAA-set standards for assessing these data.[16] When a CAPPS assessment raised security concerns the aircraft operator either screened the passenger's checked baggage using FAA-

[11] *Id.* at section 3.19. The *Commission* noted that the U.S. Customs Service (now U.S. Customs and Border Protection) successfully used such a system to better focus its resources and attention.
[12] The FAA implemented CAPPS pursuant to its general authority to prescribe regulations "to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy." 49 U.S.C. 44903(b).
[13] *See Report* at section 3.24.
[14] *See* FAA Notice of Proposed Rulemaking, Security of Checked Baggage on Flights Within the United States, 64 FR 19220, 19221 (April 19, 1999).
[15] These evaluation criteria were reviewed by the Department of Justice, *id.* at 19224-25, and implemented in consultation with aircraft operators.
[16] *Id.* FAA funds subsidized a substantial portion of the aircraft operators' cost for development of the core CAPPS system, which was provided to eight lead operators (six separate Computer Reservation Systems), all smaller operators associated with the lead operators (*e.g.,* regional feeder airlines), plus 19 other regional and national aircraft operators that collectively served approximately 95 percent of domestic airline passengers. *Id.* at 19222.

certified explosives detection equipment, or matched the bag to the passenger to ensure that the passenger's checked baggage was not transported aboard an airplane unless that passenger was aboard the same airplane and flight.

TSA was created in 2001 with the enactment of the Aviation and Transportation Security Act (ATSA),[17] and assumed responsibility for the CAPPS program from the FAA.[18] CAPPS continued to be operated by U.S. aircraft operators pursuant to the TSA-mandated Aircraft Operator Standard Security Program (AOSSP). Under this program, and prior to the implementation of Secure Flight, airlines were required to check passenger reservation data against watch lists. A CAPPS assessment indicating risk above a pre-set threshold required enhanced screening for passengers who were not on a watch list. For those passengers requiring additional screening as a result of their CAPPS assessment, the aircraft operator added the additional screening instruction to the boarding pass and TSA would perform the additional screening. As with the FAA, TSA did not receive the underlying PNR or associated reservations information. The additional screening included enhanced physical searches of individuals and their carry-on bags at the checkpoint.

[17] Pub.L. 107–71, 115 STAT. 597 (Nov. 19, 2001).

[18] In section 136 of ATSA (codified at 49 U.S.C.44903(j)(2)(C)), Congress directed that aircraft operators use CAPPS or any successor system to screen all aircraft passengers, not just those who are checking bags. *See also* TSA Notice of rulemaking status, Security of Checked Baggage on Flights Within the United States; Certification of Screening Companies, 67 FR 67382, 67383 (Nov. 5, 2002). In addition, ATSA continued in effect all "orders, determinations, rules, [and] regulations" of the FAA "until modified, terminated, superseded, set aside, or revoked in accordance with law by the [TSA Administrator], any other authorized official, a court of competent jurisdiction, or operation of law." *See* ATSA, section 141(b). ATSA also explicitly recognized the continuance of CAPPS when it exempted CAPPS from the requirement that the screening of passengers and property before boarding flights originating in the United States be carried out by a Federal Government employee. *See* 49 U.S.C. 44901(a).

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) was enacted in December 2004.[19] Section 4012(a)(1)-(2) of IRPTA directed TSA and DHS to assume the function of comparing aircraft operator passenger information to data in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC) from aircraft operators.[20] TSA promulgated its Secure Flight Program regulations consistent with this statutory directive.[21] By November 2010, TSA fully assumed the watch list matching function from aircraft operators and air carriers in Secure Flight. Since that time, CAPPS has not been used to determine whether additional screening is warranted for certain passengers. Notably, however, IRTPA did not remove or amend the statutory requirement for aircraft operators to use CAPPS. Accordingly, the statutory and regulatory authorities for the use of CAPPS remain.

Use of CAPPS Assessments in Secure Flight Risk-Based Analysis

TSA plans to incorporate a CAPPS assessment generated by aircraft operators into its Secure Flight risk-based analysis of passenger and other prescreening data as part of ongoing efforts to enhance aviation security by identifying appropriate security screening for aviation travelers.[22] The CAPPS assessments are designed to enhance

[19] Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004). A genesis for IRPTA was the report of the The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), which recommended that TSA perform watch list matching using the "larger set of watch lists maintained by the Federal Government," and that screening issues associated with CAPPS be elevated for high-level attention and addressed promptly by the government. *See Final Report of the National Commission on Terrorist Attacks Upon the United States,* page 393 (July 22, 2004).

[20] The TSC maintains the Federal Government watch lists, including the terrorism watch list known as the TSDB. 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.

[21] 73 FR 64018 (Oct. 28, 2008).

[22] For a discussion of Secure Flight risk-based analysis, see the September 10, 2013 Secure Flight SORN

TSA's analysis of passenger security risk and enable TSA to make better passenger risk decisions. The incorporation of a CAPPS assessment into the Secure Flight risk-based analysis program with Secure Flight Passenger Data (SFPD) and other prescreening data is consistent with Congress's direction in ATSA to use CAPPS in passenger screening. CAPPS assessments generated by aircraft operators continue to rely on information collected by those operators in the ordinary course of business. Secure Flight does not receive the underlying data that are used for the CAPPS assessment.[23]

TSA has taken a number of steps to review the security value of CAPPS data including evaluating whether certain CAPPS data are indicative of low-risk passengers. First, TSA worked with its airline partners to re-assess the security value of the individual CAPPS data elements. This effort resulted in refining CAPPS data elements. Second, TSA engaged the Civil Aviation Threat Working Group (CATWG), which is composed of analysts from various Federal Government agencies and led by a representative from the National Counterterrorism Center, to provide its assessment of the security value of CAPPS data. The CATWG provided its report of findings and recommendations in September 2013, which further refined the security value assigned to CAPPS data elements. Third, TSA asked the Homeland Security Studies and Analysis Institute[24] (a federally-funded research and development center) to review its approach to risk-based security screening including the use of CAPPS assessments. In March 2014, the Institute

---

update at 78 FR 55270, and the Privacy Impact Assessment for Secure Flight, DHS/TSA/PIA-018(f) (Sept. 4, 2013), found at http://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf .

[23] TSA, however, remains authorized to obtain such data for transportation security purposes under TSA's general compliance and enforcement authorities, such as TSA's authority to inspect aircraft operators to ensure compliance with security programs and TSA regulations (49 U.S.C.114(f)(7), 49 C.F.R. 1544.3); and TSA's authority to issue subpoenas and orders for the production of information (49 U.S.C. 40113(a) and 46104, 49 C.F.R. 503.203(a)). TSA also collects the SFPD required to be provided under the Secure Flight Rulemaking.

[24] *See* www.homelandsecurity.org.

endorsed TSA's approach for conducting Secure Flight risk-based analysis and recommended that TSA continue to strengthen this analysis by including CAPPS assessments. Finally, TSA reviewed its plans to use CAPPS assessments with senior officials from the Department of Homeland Security Offices of Privacy, Civil Rights and Liberties, and General Counsel. TSA further refined the security value assigned to CAPPS data elements based on input from these offices. These offices found that CAPPS assessments may be used as part of the Secure Flight risk-based analysis while also protecting passengers' privacy, civil rights, and civil liberties. In addition, these DHS offices will review CAPPS operations on an on-going basis, including the risk value assigned to individual CAPPS data elements, to assure CAPPS's continued security value, its connection to evolving security threat information, and its adherence to privacy, civil rights, civil liberties, and legal principles.

Currently, the Secure Flight passenger prescreening system has watch lists of high-risk individuals and uses these lists to issue boarding pass printing results, e.g., selectee screening or "do not board" instructions. TSA also has lists of low-risk individuals who have been issued known traveler numbers (KTN)[25] that makes them eligible for expedited screening. These individuals may receive a boarding pass printing instruction that enables them to use TSA Pre✓® lanes.[26] TSA also uses risk-based analysis of SFPD and other prescreening data to make screening determinations (e.g., to

[25] A Known Traveler Number means "a unique number assigned to an individual for whom the Federal government has conducted a security threat assessment and determined does not pose a security threat." 49 C.F.R. 1560.3.

[26] Passengers who are eligible for expedited screening are referred to a TSA Pre✓® lane where they typically are permitted to leave on their shoes, light outerwear, and belt, to keep their laptop in its case, and to keep their 3-1-1 compliant liquids/gels bag in a carry-on. TSA Pre✓® lanes are available at more than 118 airports nationwide. *See* http://www.tsa.gov/tsa-precheck/airlines-airports.

determine whether a passenger is eligible for expedited screening). The addition of CAPPS assessments to existing Secure Flight risk-based analysis will strengthen the risk assessment and increase the confidence level in the determination that a passenger is a lower risk and eligible for expedited screening.[27]

The CAPPS assessment that a passenger receives for any given flight may change on the next flight because of the range of CAPPS data and the associated security risks and benefits.

After these changes are implemented, passengers who are a match to a watch list will continue to receive appropriate enhanced screening. For all other passengers, the Secure Flight passenger prescreening computer system conducts a risk-based analysis of passenger data using: 1) the SFPD (including KTN) that TSA already receives from aircraft operators pursuant to Secure Flight regulations; 2) the CAPPS assessments; 3) frequent flyer designator codes that aircraft operators submit to TSA; and 4) other prescreening data available to TSA. The Secure Flight risk-based analysis determines whether passengers receive expedited, standard, or enhanced screening, and the results are indicated on the passenger's boarding pass.

No one will be denied the ability to fly or to enter the sterile area of an airport based solely on the results of the Secure Flight risk-based analysis, including the use of a CAPPS assessment in that analysis.

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,

[27] Another potential outcome of Secure Flight risk-based analysis is that the addition of a CAPPS score may result in a passenger receiving standard screening who otherwise may have been eligible for expedited screening, or receiving enhanced screening instead of standard screening.

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 from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines "individual" as 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:

DHS/TSA-019 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 may also be maintained at

the secured facilities of contractors or other parties performing functions under the Secure Flight program.

Categories of individuals covered by the system:

(a) Individuals who attempt to make reservations for travel on, who have traveled on, or who 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 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 by other means; and

(f) Individuals who are identified as Known Travelers for whom the Federal Government conducted a security threat assessment and determined that they 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 or verification code obtained from aircraft operators, and itinerary); records containing assessments generated by aircraft operators under the Computer-Assisted Passenger Prescreening System (CAPPS); 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 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 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 are 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 is also used to identify individuals who are lower-risk and therefore may be eligible for

expedited security screening at the airport checkpoints. 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, 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 (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 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 or her official capacity, or (c) any employee or former employee of DHS in his or 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, 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, 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 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 a potential match to a watch list are 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 are retained for seven years after the completion of the individual's directional travel itinerary. Records relating to an individual determined to be a confirmed watch list match are 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, are deleted or destroyed when superseded by an updated list.

System manager 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.

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 C.F.R. 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 (Jan. 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 such as 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 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 or created

from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records of 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.

Dated: December 10, 2014.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[FR Doc. 2014-30856 Filed 01/02/2015 at 8:45 am; Publication Date: 01/05/2015]