[4910-62-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2004-19160]

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

AGENCY: Transportation Security Administration (TSA), Department of Homeland Security (DHS).

ACTION: Notice to establish system of records; request for comments.

SUMMARY: TSA is establishing one new system of records under the Privacy Act of 1974, known as "Secure Flight Test Records." TSA will use information in the system to test the new Secure Flight program, which has been designed to assist TSA in preventing individuals known or suspected to be engaged in terrorist activity from boarding domestic passenger flights. Under this new program, TSA will compare the identifying information of airline passengers contained in passenger name records (PNRs) to the identifying information of individuals in the Terrorist Screening Database of the Terrorist Screening Center (TSC).

During the testing period for the new Secure Flight program, TSA will also conduct a separate test of the use of commercial data to determine its effectiveness in identifying passenger information that is inaccurate or incorrect. TSA does not assume that the result of comparison of passenger information to commercial data is determinative of information accuracy or the intent of the person who provided the passenger information.

For purposes of testing both the new Secure Flight program and the use of

filed: 9/21/04 12:5[illegible] pm pub: 9/24/04

commercial data to validate the accuracy of passenger-provided information, TSA will collect a limited set of historical PNRs from domestic airlines.

TSA invites comments on this notice. A further Privacy Act notice will be published in advance of any active implementation of the Secure Flight program.

DATES: This notice is effective September 24, 2004 ~~[Insert date of publication in the Federal Register]~~. The routine uses described in this notice are effective October 25, 2004 ~~[Insert 30 days after date of publication in the Federal Register]~~. Comments are due by October 25, 2004 ~~[Insert date 30 days after publication in the Federal Register]~~.

ADDRESSES: You may submit comments, identified by TSA docket number to this document, using any one of the following methods:

Comments Filed Electronically: You may submit comments through the docket web site at http://dms.dot.gov. Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477), or you may visit http://dms.dot.gov.

You also may submit comments through the Federal eRulemaking portal at http://www.regulations.gov.

Comments Submitted by Mail, Fax, or In Person: Address or deliver your written, signed comments to the Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590-0001; Fax: 202-493-2251.

Comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI) should not be submitted to the public regulatory docket.[1] Please submit such comments separately from other comments on the document. Comments containing trade secrets, confidential commercial or financial information, or SSI should be appropriately marked as containing such information and submitted by mail to Marisa Mullen, Senior Rulemaking Analyst, Office of the Chief Counsel, TSA-2, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220.

Reviewing Comments in the Docket: You may review the public docket containing comments in person in the Dockets Office between 9:00 a.m. and 5:00 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the NASSIF Building at the Department of Transportation address above. Also, you may review public dockets on the Internet at http://dms.dot.gov.

FOR FURTHER INFORMATION CONTACT: Privacy Office, Department of Homeland Security, Washington, DC 20528; Phone: 202-282-8000, Fax: 202-772-5036.

SUPPLEMENTARY INFORMATION:

Availability of Notice

You can get an electronic copy using the Internet by--

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (http://dms.dot.gov/search);

(2) Accessing the Government Printing Office's web page at http://www.access.gpo.gov/su_docs/aces/aces140.html; or

[1] See 49 CFR 1520.5 for a description of SSI material.

(3) Visiting TSA's Law and Policy web page at http://www.tsa.dot.gov/public/index.jsp.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this notice.

Background

TSA currently performs passenger and baggage screening with screening personnel and equipment at the nation's airports. This screening is supplemented by a system of computer-based passenger screening known as the Computer-Assisted Passenger Prescreening System (CAPPS), which is operated by U.S. aircraft operators. CAPPS analyzes information in passenger name records (PNRs) using certain evaluation criteria in order to determine whether a passenger or his property should receive a higher level of security screening prior to boarding an aircraft. A PNR is a record that contains detailed information about an individual's travel on a particular flight, including information provided by the passenger when making the flight reservation. Though the content of PNRs varies among airlines, PNRs may include, among other information: (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. Operationally, CAPPS is not a single system. CAPPS is programmed into the separate computer systems through which airline passenger reservations are made.

Passenger prescreening also involves the comparison of identifying information of airline passengers against lists of individuals known or suspected of posing a threat to civil aviation or national security. Aircraft operators

currently carry out this function, using lists provided by TSA. Because the lists are provided in an unclassified form, the amount of information they include is limited.

After a lengthy review of the initial plans for a successor system to CAPPS, and consistent with a recommendation of the National Commission on Terrorist Attacks upon the United States (9/11 Commission), the Department of Homeland Security is moving forward with a next generation system of domestic passenger prescreening, called "Secure Flight," that meets the following goals: (1) identifying, in advance of flight, passengers known or suspected to be engaged in terrorist activity; (2) moving passengers through airport screening more quickly and reducing the number of individuals unnecessarily selected for secondary screening; and (3) protecting passengers' privacy and civil liberties fully.

Secure Flight Description

Secure Flight will involve the comparison of information in PNRs for domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), to include the expanded TSA No-Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity. TSA will apply, within the Secure Flight system, a streamlined version of the existing CAPPS rule set related to suspicious indicators associated with travel behavior, as identified in passengers' itinerary-specific PNR. This should provide a security benefit, while at the same time improving the efficiency of the pre-screening process and reducing the number of persons selected for secondary screening. TSA will also build a "random" element into the new program to protect against those who might seek to

reverse engineer the system.

The Secure Flight program is fully consistent with the recommendation in the final report of the 9/11 Commission, which states at page 392:

> "[I]mproved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by TSA and it should utilize the larger set of watch lists maintained by the Federal Government. Air carriers should be required to supply the information needed to test and implement this new system."

Expansion of these lists to include information not previously included for security reasons will be possible as integration and consolidation of various data maintained by the TSC is completed and the U.S. Government assumes the responsibility for administering the watch list comparisons. Secure Flight will automate the vast majority of watch list comparisons; will allow TSA to apply more consistent procedures where automated resolution of potential matches is not possible; and will allow for more consistent response procedures at airports for those passengers identified as potential matches.

Secure Flight Testing Phase

Secure Flight represents a significant step in securing domestic air travel and safeguarding critical terrorism-related national security information. It will dramatically improve the administration of comparisons of passenger information with data maintained by TSC and will reduce the long-term costs to air carriers and passengers associated with maintaining the present system, which is operated individually by each air carrier that flies in the United States.

However, such comparisons will not permit TSA to identify passenger information that is incorrect or inaccurate. For this reason and on a very limited basis, in

addition to testing its ability to compare passenger information with data maintained by TSC, TSA will also test the use of commercial data to determine if this approach is effective in identifying passenger information that is incorrect or inaccurate. This test will involve commercial data aggregators who provide services to the banking, home mortgage and credit industries. Testing of these procedures will be governed by strict privacy and data security protections. TSA will not store the commercially available data that would be accessed by commercial data aggregators. TSA will use this test of commercial data to determine whether such use: (1) could accurately identify when passenger information is inaccurate or incorrect; (2) would not result in inappropriate differences in treatment of any protected category of persons; and (3) could be governed by data security safeguards and privacy protections that are sufficiently robust to ensure that commercial entities or other unauthorized entities do not gain access to passenger personal information, or to ensure that the Federal Government does not gain access inappropriately to certain types of sensitive commercial data.

Furthermore, TSA will defer any decision on how commercial data might be used in its prescreening programs, such as Secure Flight, until the completion of the test period, assessment of the test results, and publication of a subsequent System of Records Notice under the Privacy Act announcing the intended use of such commercial data.

Sources of Information Contained in the Secure Flight System

In order to obtain the passenger information necessary to test the Secure Flight program, TSA proposes to issue an order to all domestic aircraft operators directing them to submit a limited set of historical PNRs to TSA that cover commercial scheduled domestic flights. The order covers PNRs with domestic flight segments completed in the

month of June 2004. However, the order will exclude those PNRs with flight segments occurring after June 30, 2004. The purpose of this limitation is to ensure that during the test phase, TSA does not obtain any information about future travel plans of passengers on domestic flights. The order also excludes flight segments of PNRs for travel to or from the United States.

Privacy Practices; Secure Flight Testing Phase

Testing and the eventual implementation of the Secure Flight program will be governed by stringent privacy protections, including data security mechanisms and limitations on use, strict firewalls, and data access limitations between the government and commercial entities. These can be reviewed in TSA's Privacy Impact Statement on Secure Flight (found at the DHS Privacy Office website at www.dhs.gov) and also published in today's Federal Register. It is anticipated that the test duration may be as long as 30 days. Data from the test will not be transmitted to airport screeners or used for screening purposes.

Upon completion of the testing phase, and before Secure Flight is operational, TSA will establish comprehensive passenger redress procedures and personal data and civil liberties protections for the Secure Flight program. TSA is firmly committed to protecting individuals' privacy, both on a policy level and in keeping with applicable legal requirements. TSA is committed to providing access to the information that is contained in the Secure Flight Test Records system to the greatest extent feasible consistent with national security concerns. As detailed below, passengers can request a copy of most information contained about them in the system from TSA. TSA is working with the National Archives and Records Administration to obtain approval of a

records retention and disposal schedule to cover records in the Secure Flight system. TSA will propose to establish a short retention schedule for records in the Secure Flight Test Records system.

Impact on Traveling Public

At this point, the Secure Flight program is in a developmental and testing stage. TSA will not use the results of its testing for any purpose other than analysis of the efficacy of the program. Therefore, during this test phase, Secure Flight is expected to have no impact on the traveling public. However, if an indication of terrorist or possible terrorist activity is revealed during the test phase, appropriate action will be taken, to include possibly providing information in the system of records to relevant law enforcement agencies.

System of Records

DHS/TSA 017

System name:

Secure Flight Test Records

Security Classification:

Classified, sensitive

System Location:

Records are maintained at the Office of National Risk Assessment, Transportation Security Administration (TSA), Department of Homeland Security, P.O. Box 597, Annapolis Junction, MD 20701-0597, and at the Office of National Risk Assessment facility in Colorado Springs, Colorado.

Categories of Individuals Covered by the System:

Individuals traveling within the United States by passenger air transportation; and individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

Categories of Records in the System:

(a) Passenger Name Records (PNRs) obtained from aircraft operators, the specific contents of which often vary by aircraft operator;

(b) Information obtained from the Terrorist Screening Center about individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

(c) Authentication scores and codes obtained from commercial data providers; and

(d) Results of comparisons of individuals to data obtained from the Terrorist Screening Center.

Authority for Maintenance of the System:

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

Purpose(s):

The system will be used to test the Secure Flight program. The purpose of the program is to enhance the security of domestic air travel by identifying passengers who warrant further scrutiny prior to boarding an aircraft. To identify those passengers, TSA will compare PNR data with information obtained from the Terrorist Screening Center about individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

The Secure Flight test also will involve the use of a streamlined version of the rule set related to suspicious indicators associated with travel behavior, as identified in passengers' itinerary-specific PNR under the existing computer-assisted passenger prescreening system (CAPPS) currently used by aircraft operators.

The System of Records will also be used to perform limited and separate testing of the efficacy of using commercial data to identify passenger information that is incorrect or inaccurate.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses:

(1) To the Federal Bureau of Investigation where TSA becomes aware of information that may be related to an individual identified in the Terrorist Screening Database as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

(2) To contractors, grantees, experts, consultants, or other like persons when necessary to perform a function or service related to the Secure Flight program or the system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended.

(3) To the Department of Justice (DOJ) or other Federal agency in the review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which TSA exercises jurisdiction or when conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) TSA; or (b) any employee of TSA in his/her official capacity; or (c) any employee of TSA in his/her individual capacity, where DOJ or TSA has agreed to represent the employee; or (d) the

United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and TSA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records.

(4) 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.

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

(6) To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

Disclosure to consumer reporting agencies:

None.

Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records in the System:

Storage:

Records are stored electronically at the TSA Office of National Risk Assessment (ONRA) in a secure facility. 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.

Retrievability:

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

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable ONRA, TSA, and DHS automated systems security and access policies. Access to the computer system containing the records in this system of records is limited and can be accessed only by those individuals who require it to perform their official duties. The system also maintains a real-time auditing function of individuals who access the system. Classified information is appropriately stored in a secured facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information.

Retention and Disposal:

TSA is working with the National Archives and Records Administration to obtain approval of a records retention and disposal schedule to cover records in the Secure Flight system. TSA will propose to establish a short retention schedule for records in the Secure Flight Test Records system.

System Manager(s) and Address:

Director, Office of National Risk Assessment, Transportation Security Administration, P.O. Box 597, Annapolis Junction, MD 20701-0597.

Notification Procedures:

Pursuant to 5 U.S.C. 552a(k), this system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual.

Record Access Procedures:

Although the system is exempt from record access procedures pursuant to 5

U.S.C. 552a(k), DHS has determined that all persons may request access to information about them contained in a PNR by sending a written request to the TSA Privacy Officer, Transportation Security Administration (TSA-9), 601 South 12th Street, Arlington, VA 22202.

To the greatest extent possible and consistent with national security requirements, such access will be granted. Individuals requesting access must comply with the Department of Homeland Security Privacy Act regulations on verification of identity (6 CFR 5.21(d)). Individuals must submit their full name, current address, and date and place of birth. You must sign your request and your signature must either be notarized or submitted by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

Contesting Record Procedures:

A passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request to the TSA Privacy Officer, Transportation Security Administration (TSA-9), 601 South 12th Street, Arlington, VA 22202. The request should include the requestor's full name, current address, and date and place of birth, as well as a copy of the record in question, and a detailed explanation of the change sought. If the TSA Privacy Officer cannot resolve the matter, further appeal for resolution may be made to the DHS Privacy Officer. While the Privacy Act does not cover non-U.S. persons, such persons will still be afforded the same access and redress remedies.

Record Source Categories:

Information contained in the system is obtained from U.S. aircraft operators, other

Federal agencies, including Federal law enforcement and intelligence agencies, and commercial data providers.

Exemptions Claimed for the System:

Portions of this system are exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

Issued in Arlington, VA, on SEP 21 2004.

Lisa S. Dean,

Privacy Officer.