[4910-62]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Docket No. DHS/TSA-2003-1

Privacy Act of 1974: System of Records

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

ACTION: Notice of Status of System of Records; Interim Final Notice; Request for Further Comments.

SUMMARY: The Transportation Security Administration (TSA) proposed in January 2003 to establish a new system of records under the Privacy Act, known as "Passenger and Aviation Security Screening Records." This system of records would be established primarily to support the development of a new version of the Computer Assisted Passenger Prescreening System, or "CAPPS II." This notice is to inform the public that substantial comments were received in response to the prior Privacy Act notice (68 FR 2101, January 15, 2003); that significant changes have been made to date to the proposed CAPPS II system and to the CAPPS II Privacy Act notice in light of these comments; that limited developmental technical testing will occur with test data, including personal information on U.S. persons available from commercial databases, including those within and affiliated with the travel industry; and that concerns raised will continue to be considered during the testing and evaluation periods. Additional comments are sought on the modifications made to this Privacy Act notice. A further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system.

DATES: This notice is effective on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Comments due on [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Please address your comments to the Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528. You must identify the docket number DHS/TSA-2003-1 at the beginning of your comments, and you should submit two copies of your comments. You may also submit comments via email at privacy@dhs.gov. Please reference the docket number DHS/TSA-2003-1 in the subject line of the email. If you wish to receive confirmation that DHS received your comments, please include a self-addressed, stamped postcard. DHS will make the comments available online at www.dhs.gov.

FOR FURTHER INFORMATION CONTACT: Privacy Office, Department of Homeland Security, Washington, DC 20528. Phone: 202-282-8000. Fax: 202-772-9738.

SUPPLEMENTARY INFORMATION:

Background

While still a part of the Department of Transportation, in January 2003, the Transportation Security Administration (TSA) proposed establishing a new system of records under the Privacy Act, known as "Aviation Security Screening Records." TSA intends to use this system of records to facilitate TSA's passenger and aviation security screening program under the Aviation and Transportation Security Act. TSA intends to use the CAPPS II system to conduct risk assessments to ensure passenger and aviation security.

Prior to March 1, TSA was an operating administration within the Department of Transportation (DOT). While part of the DOT, TSA published for public comment proposed system of records DOT/TSA 010. See 68 FR 2101 and 2002, Jan. 15, 2003. On March 1, 2003, TSA became a component of the Department of Homeland Security (DHS) and is now continuing work towards the system of records DHS/TSA 010.

Substantial comments were received in response to the prior Privacy Act notice. Those comments can be reviewed online at http://dms.dot.gov/, by entering the docket number "1437" under "Simple Search." Significant changes have been made to date to the proposed CAPPS II system in light of these comments, and the comments and concerns raised will continue to be considered during the testing and evaluation periods. Accordingly, we are publishing an Interim Final Notice of System of Records, modified to address public comment thus far, which is effective for and applicable to the internal test activity described herein. With the publication of this notice, internal systems testing will begin, using this System of Records.

The CAPPS II system is still under consideration and development and certain elements of the technological systems are proposed for testing with attention to the issues raised in the comments received, particularly the accuracy, efficiency, and privacy impact of the proposed CAPPS II system. Results of the current technological tests, as well as the comments received, will inform the design of the final CAPPS II system. A further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system for real-time passenger screening.

Proposed CAPPS II system

TSA is establishing this system of records, now entitled "Passenger and Aviation Security Screening Records," to support the function of TSA's CAPPS II system. CAPPS II is intended to conduct risk assessments and authentications for passengers traveling by air to, from or within the United States.

Sources of Information Contained in the CAPPS II System; Process Flow

Under the proposed CAPPS II system, TSA will obtain electronically, either from airlines or from Global Distribution Systems, a passenger's "passenger name record" (PNR) as collected from the passenger by a reservation system. PNR includes the routine information collected at the time a passenger makes a flight reservation. A PNR may include each passenger's full name, home address, home telephone number and date of birth, as well as some information about that passenger's itinerary. No additional information beyond this data is required to be collected from passengers for the operation of CAPPS II.

The CAPPS II system will access PNRs prior to the departure of the passenger's flight. Selected information will be securely transmitted to commercial data providers, for the sole purpose of authenticating passenger identity. This authentication will be accomplished not by a permanent co-mingling of data, but merely by the commercial data providers transmitting back to TSA a numeric score, which is an indication of the percentage of accuracy of the match between the commercial data and the data held by TSA. This will enable TSA to have a reasonable degree of confidence that each passenger is who he or she claims to be. TSA recognizes that inaccuracies in the commercial data may exist and that the CAPPS II system must allow for and compensate for such

inaccuracies; this test phase is intended to test and further develop such capabilities in the system.

Commercial data providers will receive a limited amount of identifying information from TSA with regard to each passenger, and will provide TSA with an authentication score and code indicating a confidence level in that passenger's identity. The commercial data providers will not provide TSA with any additional information about the individual. They will not acquire ownership of the data, nor will they be permitted to retain the data in any commercially usable form. TSA will not permit the commercial data providers to use this data for any purpose other than in connection with the CAPPS II program. Importantly, the commercial data provider will not retain information about the response they provide to TSA in any record about the individual that they maintain. Further, no persistent link between an individual's records in the private sector and that person's records within the CAPPS II system will be created.

Once CAPPS II has authenticated a passenger's identity, it will conduct its risk assessment. The risk assessment function is conducted internally within the U.S. government and will determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations. National security information from within the federal government, as well as information reflecting federal officials with high levels of security clearance, will be part of this analysis function.

After the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence may also be analyzed and applied in the context of this system. At or after such time as the system becomes operational, where there is an indication of a serious

violation of criminal law (as described in the Routine Use section, below), such information may be shared between law enforcement agencies and the Department of Homeland Security and appropriate action may be taken. It is further anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program at such time as both programs become fully operational, in order that the processes at both border and airport points of entry and exit are consistent. Any such linkages will be performed in full compliance with the Privacy Act of 1974, including any applicable requirement for additional notice.

It is important to note the CAPPS II system is designed to determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations, including both foreign and domestic terrorist organizations.

Lastly, it is anticipated that dynamic inputs to the system from intelligence sources will allow the system to respond to current threat conditions and information on a timely basis.

Impact on Traveling Public

Based upon the combination of information derived from commercial sources, national security sources, and dynamic intelligence data, each traveling passenger will be identified with a "risk score," indicating whether that person's information leads to a determination of low, high, or unknown risk to passenger and aviation security.

In the vast majority of cases, passengers will be identified as "low risk," and will simply pass through the ordinary airport security screening process to their flights.

In a small percentage of cases, passengers may be found to present an elevated, uncertain or "unknown risk" of terrorism. In such cases, the passengers in question will

be subjected to heightened security screening prior to boarding their flights. Once these passengers have successfully completed this screening, they will proceed to their flights in the normal manner; they will not be penalized, nor will additional information about them be retained within the CAPPS II system.

Where a passenger is found to be "high risk"--to have identifiable links to terrorism, law enforcement or other appropriate authorities will be notified for appropriate action. It is anticipated that the number of passengers so identified as high risk will be extremely small, but any so identified may be critically significant in the context of homeland security.

Privacy Practices

The Department of Homeland Security is committed to working with airlines and the travel industry to provide greater understanding and awareness of the purposes for and the scope of CAPPS II. Consistent with fair information principles, The Department of Homeland Security will work towards adequate notice to the passenger when that passenger provides information that will be used for security purposes.

Further, DHS is committed to providing access to the information that is contained in the CAPPS II 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 the CAPPS II passenger advocate. Further, DHS is currently developing a robust review and appeals process, to include the DHS privacy office.

<u>System Testing of CAPPS II</u>

At this point, partly in response to concerns raised by the public about the viability and function of the CAPPS II program, TSA plans to test certain portions of the system, including the technological communications between the CAPPS II system and the various data sources, as well as the identity authentication programs. These tests are intended to respond to public concerns about speed, accuracy, and efficiency of the system. Testing will be concerned with the accuracy of public and private information contained in the system, particularly in the authentication process; the speed of response of the system; identifying and minimizing the data necessary to effectively conduct the operation of CAPPS II; and the overall ability of the system to identify risk levels effectively. During these tests, TSA will use and retain PNR data for the duration of the test period. It is anticipated that the test duration may be as long as 180 days. A persistent link to law enforcement databases will not be created for the purposes of the test, nor will data from the test be transmitted to airport screeners or used for screening purposes during the test period. If, however, an indication of terrorist or potential terrorist activity is revealed during the test period, appropriate action will be taken. A final Privacy Act notice will be published before the CAPPS II system is deployed.

Public Comments

TSA received well over 200 comments on proposed system of records DOT/TSA 010 – "Aviation Security Screening Records." Comments generally expressed concern that the proposed CAPPS II system was too broad in scope and would prove invasive to passengers' privacy. Several commenters stated that the proposed system of records contained too wide a variety of personal information and allowed for the collection and retention of too much information on private citizens. Commenters also expressed

concern about the quality of data contained in commercial databases, and that such data could be used to prevent them from traveling by air. Some commenters stated that the proposed retention of data for up to 50 years was too long. Another concern expressed was the broad variety of "routine uses," which, in the opinion of some commenters, allowed TSA far too much discretion to disseminate private information. One commenter expressed the view that the CAPPS II system would lead to the misallocation of security resources.

TSA respects the concerns raised by commenters and has modified the proposed system of records to address many of those concerns. The test of the technological systems responds, in part, to concerns of accuracy, efficiency, and effectiveness, which are among the underpinnings of evaluating such a system's impact on an individual's privacy. Any subsequent modifications to the system that arise from the knowledge gained from these tests will be published in a subsequent notice.

This system notice reduces the extent to which TSA will maintain or disseminate personal information on airline passengers. At the same time, however, TSA must ensure that it collects information sufficient to carry out its security screening functions in an efficient and effective manner, consistent with its legislative mandate to ensure passenger and aviation security. In establishing the parameters of the Passenger and Aviation Security Screening Records system, TSA has attempted to address privacy interests of passengers and the public, while simultaneously working towards increased transportation security.

Responses to Comments; Modifications to System

As discussed above, several commenters objected to the amount of personal information that TSA proposed to maintain in the proposed system of records. Under this system notice, TSA will not retain significant amounts of personal information after completion of a passenger's itinerary. TSA eliminated language in the proposed notice that could be read to mean that TSA will collect and maintain large amounts of information about individuals.

Concerns have been raised about the retention of data after a passenger's travel. In response, TSA is working to minimize the length of time any data about passengers will be retained. In response to concerns, the proposal to maintain information about certain individuals for up to 50 years has been deleted. Under the final CAPPS II program, when active, it is anticipated that TSA will delete all records of travel for U.S. citizens and lawful permanent resident aliens not more than a certain number of days after the safe completion of their travel itinerary. At this time, the amount of information about non-US persons and the length of time for which that information will be kept when the CAPPS II system is deployed are matters still under consideration.

The limited test data used during the test period will be retained solely for the duration of the test; at the conclusion of the test, DHS expects that all data from the test will be destroyed, unless otherwise required by law. In either case, such data will not be included in the live activation of CAPPS II.

Commenters also objected to the broad description of the types of data to be collected from passengers. Specifically, commenters stated that there was no clear

explanation of what TSA meant by "associated data" in the reference to TSA's collection of PNR and "associated data." In response, TSA has deleted the phrase "associated data."

Some commenters objected to the large variety of different types of data that TSA proposed to maintain in the system of records. TSA has significantly reduced the variety of data to be maintained in the system. For the vast majority of passengers, the CAPPS II system, when active, will maintain only the routine information that all individuals provide when making reservations, as contained in the PNR, including full name, date of birth, home address and home phone number, to the extent available. In addition, the CAPPS II system will contain authentication scores and codes, and a TSA-generated risk assessment score. The system will also contain some information derived from governmental databases containing information on, or pertinent to, the detection of terrorists and their associates and the detection of the serious criminal violations detailed in this notice, as well as information on government officials and other persons holding security clearances or positions of trust such as not to warrant heightened scrutiny. However, in response to specific concerns regarding the use of information about an individual's creditworthiness or individual health records, TSA will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination.

Other commenters raised concerns that large numbers of people would be prevented from flying as a result of the use of inaccurate commercial records. One of TSA's primary purposes in creating this new system is to avoid the kind of miscommunication and improper identification that has, on occasion, occurred under the

systems currently in use. During the test period, TSA hopes to confirm that the use of the CAPPS II program will significantly reduce improper identification.

Routine Uses

In response to the comments received that expressed concerns about the further dissemination of passenger information, TSA has narrowed several routine uses in the proposed notice, and eliminated others in their entirety, as follows:

Proposed Routine Use 1 (to Federal, State, local, international, or foreign agencies) (now Routine Use 1) has been narrowed to pertain to specified violations of criminal law.

Proposed Routine Use 3 (now Routine Use 3) has been modified to specify immigration and intelligence agencies.

Proposed Routine Uses 4 (to individuals and organizations), 5 (to government agencies in connection with employment, contract or benefit matters) and 6 (to news media) have been deleted.

Proposed Routine Use 2 (now Routine Use 2) and proposed Routine Use 9 (now Routine Use 4) have been modified slightly to make the language consistent with the routine uses in other TSA systems of records. These changes are not substantive and do not expand or narrow the scope of the routine uses.

Proposed Routine Use 10 (now Routine Use 5) has been modified slightly to allow for disclosures to airports and aircraft operators only to the extent required in the interests of counterterrorism or passenger or aviation security.

Proposed Routine Use 11 (now Routine Use 6) has been modified to permit disclosure to the General Services Administration (GSA), in addition to the National Archives and Records Administration (NARA), for purposes of records management

inspections. Both GSA and NARA have the statutory authority under 44 U.S.C. 2904 and 2906 to conduct inspections or surveys of TSA records, which was not reflected in the proposed routine use. This modification corrects the omission.

DHS/TSA 010

System name:

Passenger and Aviation Security Screening Records

Security Classification:

Classified, sensitive

System location:

Records are maintained at the Transportation Security Administration (TSA), Department of Homeland Security, P.O. Box 597, Annapolis Junction, MD 20701-0597.

Categories of Individuals covered by the system:

Individuals traveling to, from or within the United States by passenger air transportation; known terrorists and individuals on terrorism watch lists; persons with outstanding federal or state warrants for crimes of violence; government officials or other persons holding requisite security clearances, positions of trust and confidence, or otherwise deemed not to require heightened scrutiny.

Categories of records in the system:

(a) Passenger Name Records (PNRs) obtained from airlines, Global Distribution Systems and Computer Reservation Systems (the specific contents of PNRs often vary by airline, but will include at least the following passenger information: full name, date of birth, home phone number, home address, and travel itinerary); other

information in PNR may include payment information, and frequent flier number (if any);

(b) authentication scores and codes obtained from commercial data providers;

(c) numerical "risk scores" generated by the CAPPS II system;

(d) watch lists and government databases containing information on known terrorists and terrorist associates, or other information pertinent to the detection of terrorists and their associates, or pertinent to the detection of outstanding state or federal warrants for crimes of violence.

(e) names of and other identifying information about government officials or other persons holding security clearance or positions of trust and confidence, such as not to warrant heightened scrutiny.

Authority for maintenance of the system:

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

Purpose(s):

The system will be used to facilitate the development, testing, and conduct of the Computer Assisted Passenger Prescreening System II (CAPPS II). The purpose of CAPPS II is to minimize threats to passenger and aviation security by determining which passengers should be afforded additional scrutiny prior to boarding an aircraft. In addition, CAPPS II is designed to determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations, including both foreign and domestic terrorist organizations, or otherwise poses a threat to passenger or aviation security.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

1) To appropriate Federal, State, local, international, or foreign agencies or authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, or order, or in accordance with law or international agreements, where DHS becomes aware of an outstanding state or federal arrest warrant for a crime of violence.

2) To contractors, grantees, experts, or consultants when necessary to perform a function or service related to the CAPPS II system or this 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 Federal, State, local, international, or foreign agencies or authorities, including those concerned with law enforcement, visas and immigration, and to agencies in the Intelligence Community, or in accordance with law or international agreements, with respect to persons who may pose a risk of air piracy or terrorism or who may pose a threat to aviation, passenger safety or national security.

4) To the Department of Justice or other Federal agencies conducting litigation, or in a proceeding before a 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 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.

5) To airports and aircraft operators, only to the extent the disclosure is deemed required for counterterrorism or passenger or aviation security purposes.

6) To the General Services Administration and the National Archives and Records Administration (NARA) in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

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 a TSA secure facility. The records are stored on magnetic disc, tape, digital media, 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, such as flight number.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable DHS automated systems security and access policies. The computer system from which records could be accessed is policy and security based, meaning access is limited to 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, and secured databases and containers and in accordance with other applicable requirements, including those pertaining to classified information.

Retention and disposal:

A request is pending for NARA approval for the retention and disposal of records in this system. For U.S. persons, (i.e., citizens and lawful permanent resident aliens), records will be deleted within a set number of days after the safe completion of the travel to which the record relates. The duration of data retention for other persons is still under consideration. Factors to be considered in determining data retention for those persons will include the extent of information required to accurately authenticate passenger identity and the amount of data available from commercial data on non-U.S. persons, relative to U.S. persons. Existing records obtained from other government agencies, including intelligence information, watch lists, and other data, will be retained for three years, or until superseded.

Passenger data used for purposes of system development and testing will be deleted upon completion of the test phase.

System manager(s) and address:

Director, CAPPS II, TSA, 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 records containing information they provided by sending a written request to the CAPPS II Passenger Advocate (P.O. Box 597, Annapolis Junction, MD 20701-0597). To the greatest extent possible and consistent with national security requirements, such access will be granted. In the case of air passengers, this data is contained in the PNR. 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. As noted above, however, in order to protect passenger privacy, PNR data is not retained for any significant time in this system. Accordingly, in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system.

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 CAPPS II Passenger Advocate, at P.O. Box 597, Annapolis Junction, MD, 20701-0597. The request should include the requestor's full name, current address and date of birth, as well as a copy of the record in question, and a detailed explanation of the change sought. If the matter cannot be resolved by the CAPPS II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office. While non-U.S. persons are not

covered by the Privacy Act, such persons will still be afforded the same access and redress remedies. These remedies for all persons will be more fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational.

Record source categories:

Pursuant to 5 U.S.C. 552a(k), this system is exempt from publishing the categories of sources of records.

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), (H), and (I), and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

Issued in Washington, D.C. on July 22, 2003.

Signature

Tom Ridge
Secretary
U.S. Department of Homeland Security