

[Filed and available for inspection with the Office of the Federal Register on May 27, 2004. To be published on June 1, 2004]

[4910-62-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2004-17982]

**Privacy Act of 1974: Systems of Records; Telecommunications Usage Detail
Records; Registered Traveler Operations Files**

AGENCY: Transportation Security Administration (TSA), DHS.

ACTION: Notice to establish two new systems of records; request for comments.

SUMMARY: The Transportation Security Administration is establishing two new system of records under the Privacy Act of 1974.

DATES: Comments due on [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Address your comments to the Docket Management System, U.S. Department of Transportation (DOT), Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590-0001. You must identify the docket number TSA-2004-17982 at the beginning of your comments, and you should submit two copies of your comments. If you wish to receive confirmation that TSA received your comments, include a self-addressed, stamped postcard.

You may also submit comments through the Internet at <http://dms.dot.gov>. Please be aware that anyone is able to search the electronic form of all comments received into any of these 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 DOT's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (Volume 65, Number 70; Pages 19477-78) or you may visit <http://dms.dot.gov>. You may also review the public docket containing comments in person at the Dockets Office between 9:00 a.m. and 5:00 p.m., Monday through Friday, except Federal holidays. The Dockets Office is on the plaza level of the NASSIF Building at the Department of Transportation at the above address.

FOR FURTHER INFORMATION CONTACT: Conrad Huygen, Privacy Act Officer, TSA Office of Information Management Programs, TSA Headquarters, West Tower, 11th Floor (TSA-17), 601 S. 12th Street, Arlington, VA 22202-4220; telephone (571) 227-1954; facsimile (571) 227-2912.

SUPPLEMENTARY INFORMATION: The Transportation Security Administration is establishing two new systems of records under the Privacy Act of 1974. The first system, Telecommunications Usage Detail Records (DHS/TSA 014), will be used to facilitate the management of telecommunications equipment within TSA, to prevent the misuse of government resources, and to serve as the basis for appropriate disciplinary action in the event government resources have been misused.

The second system, Registered Traveler Operations Files (DHS/TSA 015), will be used to conduct a Registered Traveler (RT) Pilot Program in a limited number of airports to test and evaluate the merits of the RT concept on a completely voluntary basis. RT is designed to pre-screen and positively identify volunteer travelers using advanced identification technologies and conduct a terrorist-focused background check to ensure that the volunteer is not connected to terrorists or terrorist activity. This system may

expedite the pre-boarding process for the traveler and improve the allocation of TSA's security resources on individuals who may pose a security threat. All passengers who volunteer and are deemed eligible for the RT pilot program will be required to undergo physical screening at the screening checkpoint in the selected pilot locations.

DHS/TSA 014

System name:

Telecommunications Usage Detail Records.

Security classification:

Unclassified, sensitive.

System location:

Records are maintained in the Office of Information Technology at TSA Headquarters in Arlington, Virginia and at various TSA field offices.

Categories of individuals covered by the system:

Employees and contractor personnel who use or are assigned government telephones, cell phones, facsimile machines, computers connected to the Internet, or other telecommunications equipment.

Categories of records in the system:

Records relating to the use of government telecommunications equipment; records indicating assignment of telecommunications equipment to individuals, which may include the individual's name, duty title, address, social security number, assigned equipment identifying information, and assigned phone number; and records relating to the location of government telecommunications equipment.

Authority for maintenance of the system:

5 U.S.C. 301; 49 U.S.C. 114; E.O. 9397 (Social Security Number).

Purposes:

Records are maintained to facilitate the management of telecommunications equipment, to prevent the misuse of government resources, and to serve as the basis for appropriate disciplinary action in the event government resources have been misused.

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

(1) To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to 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.

(2) To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

(3) To the Department of Justice (DOJ) or other Federal agency 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 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.

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

(6) To the Department of Justice, United States Attorney's Office, or other agency for debt collection action on any delinquent debt when circumstances warrant.

(7) To respond to a Federal agency's request made in connection with the hiring or retention of an employee, the letting of a contract, or issuance of a grant, license or other benefit by the requesting agency, but only to the extent that the information disclosed is relevant and necessary to the requesting agency's decision on the matter.

(8) To a telecommunications company providing telecommunications support to permit servicing of the account.

(9) To third parties during the course of an investigation into violations or potential violations of relevant laws, regulations, or policies to the extent necessary to obtain information pertinent to the investigation.

Disclosures to consumer reporting agencies:

Pursuant to 5 U.S.C. 552a(b)(12), disclosures may be made from this system to consumer reporting agencies collecting on behalf of the United States Government.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in hard copy or in electronic format on a system database.

Retrievability:

Records are retrieved by name, duty title, address, social security number, equipment number, phone number, or other assigned identifier of the individual on whom the records are maintained.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Control measures are enforced to ensure that access to sensitive information in these records, such as Social Security Numbers, is based on a “need to know.”

Retention and disposal:

Records in this system will be retained in accordance with a schedule to be approved by the National Archives and Records Administration.

System manager(s) and address:

Telecommunications Equipment Manager, Office of Information Technology, TSA Headquarters, TSA-11, 601 S. 12th Street, Arlington, VA 22202-4220.

Notification procedure:

To determine whether this system contains records relating to you, write to the System Manager identified above.

Record access procedure:

Same as “Notification Procedure,” above. Provide your full name and a description of information that you seek, including the time frame during which the

record(s) may have been generated. Individuals requesting access must comply with the Department of Homeland Security Privacy Act regulations on verification of identity (6 CFR 5.21(d)).

Contesting record procedure:

Same as “Notification Procedure” and “Record Access Procedure,” above.

Record source categories:

Information contained in this system is obtained from employees and contractor personnel who use or are assigned government telecommunications equipment, telecommunications equipment assignment lists, call detail log entries (which include but are not limited to whom the call was made, from where the call was made, and call duration), and the results of inquiries related to the assignment of responsibility for the misuse of government telecommunications equipment or the placement of unofficial calls or transmissions.

Exemptions claimed for the system:

None.

DHS/TSA 015

System name:

Registered Traveler (RT) Operations Files.

Security classification:

Classified, sensitive.

System location:

Records will be maintained at TSA Headquarters in Arlington, Virginia, at other authorized TSA or DHS secure facilities as necessary, and at a digital safe site managed by a government contractor.

Categories of individuals covered by the system:

(a) Individuals who voluntarily apply to participate in the RT Pilot Program, who agree to provide personal information to TSA that may be used as part of a security assessment, and who may or may not meet the eligibility criteria as determined by TSA;

(b) Authorized Federal law enforcement officers (LEOs); and (c) Individuals who participate in the Federal Flight Deck Officer (FFDO) program.

Categories of records in the system:

Information in the system includes some or all of the following: full name, current home address, current home phone number, current cell phone number (if applicable), social security number, date of birth, place of birth, nationality, gender, prior home addresses, arrival date in United States (non-U.S. citizens only), digital photo, reference biometric (i.e. fingerprint(s), iris scan, facial geometry, hand geometry, handwriting/signature, others), unique identification record number, unique token or credential serial number, security assessments, information pertaining to adjudication results, RT eligibility status, token or credential issue date, token or credential expiration date, information and data provided by Federal, State, and local government agencies and foreign governments that is necessary to conduct a security assessment to determine if an individual poses a potential threat to aviation security. Authorized Federal LEOs may have a Federal LEO code name and unique administrative code number.

Authority for maintenance of the system:

49 U.S.C. 114; Section 109(a)(3), Aviation and Transportation Security Act (ATSA), Pub.L.107-71.

Purpose(s):

The system utilized during the RT Pilot Program will facilitate the development, testing, and administration of the RT concept, including conducting security assessments on program applicants; additional security assessments may or may not be conducted on authorized LEOs, FFDOs, and other authorized government officials. The purpose of the RT pilot program is to (1) pre-screen and positively identify volunteer travelers using advanced identification technologies, including biometrics, which may expedite the pre-boarding process for the traveler and improve the allocation of TSA's security resources on individuals who may pose a security threat; (2) prevent potential threats from individuals who are impersonating Federal LEOs and seek to board commercial aircraft while armed; (3) assist in the management and tracking of the status of security assessments for applicants and those deemed eligible for the Registered Traveler Pilot Program; (4) permit the retrieval of the results of security assessments, including criminal history records checks and searches in other governmental identification systems, performed on the individuals covered by this system; (5) permit the retrieval of information from other law enforcement and intelligence databases on individuals covered by this system; and (6) identify potential threats to transportation security, uphold and enforce the law, and ensure public safety.

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

(1) To the United States Department of Transportation, its operating administrations, or the appropriate state or local agency when relevant or necessary to (a) ensure safety and security in any mode of transportation; (b) enforce safety and security related regulations and requirements; (c) assess and distribute intelligence or law enforcement information related to transportation security; (d) assess and respond to threats to transportation; (e) oversee the implementation and ensure the adequacy of security measures at airports and other transportation facilities; (f) plan and coordinate any actions or activities that may affect transportation safety and security or the operations of transportation operators; or (g) the issuance, maintenance, or renewal of a license, certificate, contract, grant, or other benefit.

(2) To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

(3) To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to 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.

(4) To airports and aircraft operators to the extent necessary to identify Registered Travelers and ensure the proper ticketing, security screening, and boarding of those passengers.

(5) To a Federal, State, local, tribal, territorial, foreign, or international agency, in response to queries regarding persons who may pose a risk to transportation or national

security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security.

(6) To the Department of State and other Intelligence Community agencies to further the mission of those agencies relating to persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; a threat to aviation safety, civil aviation, or national security.

(7) To international and foreign governmental authorities in accordance with law and formal or informal international agreement.

(8) To authorized law enforcement and other government agencies, as necessary, to conduct the security assessments and, if applicable, to facilitate payment and accounting.

(9) To the Department of Justice in review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which TSA exercises jurisdiction.

(10) To the DOJ or other Federal agency 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.

(11) 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.

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

(13) To the Attorney General of the United States or his/her official designee, when information indicates that an individual meets any of the disqualifications for receipt, possession, shipment, or transport of a firearm under the Brady Handgun Violence Prevention Act. In case of a dispute concerning the validity of the information provided by TSA to the Attorney General, or his/her designee, it shall be a routine use of the information in this system of records to furnish records or information to the national Background Information Check System, established by the Brady Handgun Violence Prevention Act, as may be necessary to resolve such dispute.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records may be stored on magnetic disc, tape, digital media, CD-ROM, bar code, magnetic stripe, optical memory stripe, disk, integrated circuit chip, and/or other approved technologies and may also be retained in hard copy format in secure file folders.

Retrievability:

Records may be retrieved by the applicant's name, unique identification record number, or other unique administrative identifier; paper records, where applicable, are retrieved alphabetically by name or other unique administrative identifier.

Safeguards:

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 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, secured databases, and containers and in accordance with other applicable requirements, including those pertaining to classified information.

Retention and disposal:

Records in this system will be retained in accordance with a schedule to be approved by the National Archives and Records Administration.

System manager and address:

Registered Traveler Program Manager, Credentialing Program Office, TSA Headquarters, TSA-19, East Tower, 601 S. 12th Street, Arlington, VA 22202-4220.

Notification procedure:

To determine if this system contains a record relating to you, write to the system manager at the address indicated above and provide your full name, current address, date

of birth, place of birth, and a description of information that you seek, including the time frame during which the record(s) may have been generated. You may also provide your Social Security Number or other unique identifier(s) but you are not required to do so. Individuals requesting access must comply with the Department of Homeland Security's Privacy Act regulations on verification of identity (6 CFR 5.21(d)).

Record access procedure:

Same as "notification procedure," above.

Contesting record procedure:

Same as "notification procedure," above.

Record source categories:

Information contained in this system may be obtained from the RT applicant, law enforcement and intelligence agency record systems, government and commercial databases, military and National Guard records, and other Department of Homeland Security systems.

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 Arlington, Virginia, on May 27, 2004.

/s/

Barry D. Walters

Director, Office of Information Management Programs

