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 September 21, 2004.

Lisa S. Dean,

Privacy Officer.

[FR Doc. 04–21479 Filed 9–21–04; 12:59 pm]

BILLING CODE 4910–62–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2004–19166]

Privacy Act of 1974: Systems of Records; Transportation Security Threat Assessment System (T–STAS); Transportation Worker Identification Credentialing (TWIC) System

AGENCY: Transportation Security Administration (TSA), DHS.

ACTION: Notice to alter two existing systems of records; request for comments.

SUMMARY: TSA is altering two existing systems of records under the Privacy Act of 1974.

DATES: Comments due on October 25, 2004.

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–2004–19166 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 a.m. and 5 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, Office of Information Management Programs, TSA Headquarters, TSA–17, 601 S. 12th Street, Arlington, VA 22202–4220; telephone (571) 227–1954; facsimile (571) 227–2906.

SUPPLEMENTARY INFORMATION: TSA is altering two existing systems of records under the Privacy Act of 1974. The first system, the Transportation Security

Threat Assessment System (DHS/TSA 002), facilitates the performance of threat assessments and employment investigations on individuals who require special access to the transportation system and was published in the **Federal Register** on August 18, 2003, as the Transportation Workers Employment Investigations System. See 68 FR 49496, 49498. The system name has been changed and the categories of individuals, categories of records, and purposes of the system expanded to cover threat assessments performed on individuals seeking flight training, temporary flight restriction waivers, and access to cargo-related infrastructure and other transportation-related activities. The routine uses have also been amended to allow for the disclosure of records related to these new activities, to include state and local transportation agencies, when compatible with the purposes for which the information was collected. TSA may now also share information with the appropriate agency when individuals pose or are suspected of posing a risk to transportation or national security. Records may also be retrieved using biometric identifiers.

The second system, the Transportation Worker Identification Credentialing (TWIC) System (DHS/TSA 012), facilitates the testing and evaluation of certain technologies and business processes associated with access control for transportation workers requiring unescorted access to secure areas of transportation facilities and was first published in the **Federal Register** on August 18, 2003. See 68 FR 49496, 49507. The system notice is being changed to reflect the expanded location of the records in the TWIC Prototype Phase and the routine uses have been amended to allow for the disclosure of records to state and local transportation agencies when compatible with the purposes for which the information was collected. TSA may now also share information with the appropriate agency when individuals pose or are suspected of posing a risk to transportation or national security. The complete revised notices of both systems of records follow.

TRANSPORTATION AND SECURITY ADMINISTRATION
DHS/TSA 002

SYSTEM NAME:

Transportation Security Threat Assessment System (T–STAS).

SECURITY CLASSIFICATION:

Classified, Sensitive.

SYSTEM LOCATION:

Records are maintained at the offices of the Transportation Security Administration (TSA) Headquarters in Arlington, Virginia. Some records may also be maintained at the offices of TSA contractors, or in TSA field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are required to undergo a security threat assessment or employment investigation in order to obtain access to the following: Transportation infrastructure or assets, such as terminals, facilities, pipelines, railways, mass transit, vessels, aircraft, or vehicles; restricted airspace; passenger baggage; cargo; or transportation-related instruction or training (such as flight training). This includes but is not limited to the following individuals:

(a) Individuals who require or seek access to airport secured, sterile, or a Security Identification Display Area (SIDA); have or seek unescorted access authority to these areas; have or seek authority to grant others unescorted access to these areas; have or seek regular escorted access to these areas; or are seeking identification that is evidence of employment at the airport.

(b) Individuals who have or are seeking responsibility for screening passengers or carry-on baggage, and those persons serving as immediate supervisors and the next supervisory level to those individuals, other than employees of the TSA who perform or seek to perform these functions.

(c) Individuals who have or are seeking responsibility for screening checked baggage or cargo, and their immediate supervisors, and the next supervisory level to those individuals, other than employees of the TSA who perform or seek to perform these functions.

(d) Individuals who have or are seeking the authority to accept checked baggage for transport on behalf of an aircraft operator that is required to screen passengers.

(e) Pilots, copilots, flight engineers, flight navigators, airline personnel authorized to fly in the cockpit, relief or deadheading crewmembers, cabin crew, and other flight crew for an aircraft operator or foreign air carrier that is required to adopt and carry out a security program.

(f) Flight crews and passengers who request waivers of temporary flight restrictions (TFRs) or other restrictions pertaining to airspace.

(g) Other individuals who are connected to the transportation industry for whom TSA conducts security threat assessments to ensure transportation security.

(h) Individuals who have or are seeking unescorted access to cargo in the transportation system.

(i) Individuals who are owners, officers, or directors of an indirect air carrier or a business seeking to become an indirect air carrier.

(j) Aliens or other individuals designated by TSA who apply for flight training or recurrent training.

(k) Individuals transported on all-cargo aircraft, including aircraft operator or foreign air carrier employees and their family members and persons transported for the flight.

CATEGORIES OF RECORDS IN THE SYSTEM:

TSA's system may contain any or all of the following information regarding individuals covered by this system: (a) Full name (including aliases or variations of spelling); (b) gender; (c) current and historical contact information (including but not limited to address information, telephone number, e-mail); (d) government issued licensing or identification information (including but not limited to social security number, pilot certificate information, including number and country of issuance, and other licensing information for modes of transportation); (e) date and place of birth; (f) name and information including contact information and identifying number (if any) of the airport, aircraft operator, indirect air carrier, maritime or land transportation operator, or other employer or entity that is employing the individual or submitting the individual's information or sponsoring the individual's background check/threat assessment; (g) physical description, fingerprint and/or other biometric identifier and photograph; (h) date, place, and type of flight training or other instruction; (i) control number or other unique identification number assigned to an individual or credential; (j) information necessary to assist in tracking submissions, payments, and transmission of records; (k) results of any analysis performed for security threat assessments and adjudications; (l) other data as required by Form FD 258 (fingerprint card) or other standard fingerprint cards used by the Federal government; (m) information provided by individuals covered by this system in support of their application for an appeal or waiver; (n) flight information, including crew status on board; (o) travel document information (including but not limited to passport information, including number and country of issuance, and current and past

citizenship information and immigration status, any alien registration numbers, and any visa information); (p) identification records obtained from the Federal Bureau of Investigation (FBI), which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the FBI's Fingerprint Identification Records System (FIRS); (q) data gathered from foreign governments or entities that is necessary to address security concerns in the aviation, maritime, or land transportation systems; (r) other information provided by Federal, State, and local government agencies or private entities; (s) the individual's level of access at an airport.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 114, 5103a, 40103(b)(3), 40113(a), 44903(b), 44936, 44939, 46105.

PURPOSE(S):

(a) Performance of security threat assessments and employment investigations that Federal statutes and/or TSA regulations authorize for the individuals identified in ''Categories of individuals covered by the system,'' above.

(b) To assist in the management and tracking of the status of security threat assessments and employment investigations.

(c) To permit the retrieval of the results of security threat assessments and employment investigations, including criminal history records checks and searches in other governmental, commercial, and private data systems, performed on the individuals covered by this system.

(d) To permit the retrieval of information from other terrorist-related, law enforcement and Intelligence databases on the individuals covered by this system.

(e) To track the fees incurred and payment of those fees by the airport operators, aircraft operators, maritime and land transportation operators, flight students, and others where appropriate for services related to security threat assessments and employment investigations.

(f) To facilitate the performance of security threat assessments and other investigations that TSA may conduct to ensure transportation security.

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, endorsement, 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 the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding individuals who pose or are suspected of posing a risk to transportation or national security.

(4) To contractors, grantees, experts, consultants, volunteers, or other like persons 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.

(5) To a Federal, State, local, tribal, territorial, foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual, or the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit.

(6) To a Federal, State, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a TSA decision concerning the hiring or retention of an employee, the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit.

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

(8) To third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request, to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication.

(9) To airport operators, indirect air carriers, aircraft operators, flight school operators, and maritime and land transportation operators or contractors about individuals who are their employees, job applicants, or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities, or provide flight training, when relevant to such employment, application, contract, or the issuance of such credentials, clearances, or acceptance for flight training.

(10) To a Federal, State, local, tribal, territorial, foreign, or international agency so that TSA may obtain information to conduct security threat assessments or employment investigations and to facilitate any associated payment and accounting.

(11) 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.

(12) 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.

(13) To the National Archives and Records Administration or other appropriate Federal agency pursuant to 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:

In electronic storage media and hard copy.

RETRIEVABILITY:

Information can be retrieved by name, social security number, identifying number of the submitting or sponsoring entity, other case number assigned by TSA or other entity/agency, biometric, or a unique identification number or any other identifying particular assigned or belonging to the individual.

SAFEGUARDS:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include some or all of the following: restricting access to those authorized with a need-to-know; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

RETENTION AND DISPOSAL:

National Archives and Records Administration approval is pending for the records in this system.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director for Compliance, Credentialing Program Office, TSA–19, 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 is collected from individuals subject to a security threat assessment or employment investigation; from aviation, maritime, and land transportation operators, flight schools, or other persons sponsoring the individual; and any other persons, including commercial entities, that may have information that is relevant or necessary to the assessment or investigation. Information about individuals is also used or collected from domestic and international intelligence sources and other governmental, private, and public databases. The sources of information in the criminal history records obtained from the FBI are set forth in the Privacy Act system of records notice ''JUSTICE/FBI–009.''

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Portions of this system are exempt under 5 U.S.C. 552a(k)(1) and (k)(2).

DHS/TSA 012

SYSTEM NAME:

Transportation Worker Identification Credentialing (TWIC) System.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATIONS:

Records will be maintained in a secure, centralized location for selected transportation facilities within three geographic regions: Delaware River and Bay, Los Angeles/Long Beach, California, and the State of Florida. Locations within the Los Angeles/Long Beach region include Carson, CA; Terminal Island, CA; Oakland, CA; San Pedro, CA; Long Beach, CA; and Los Angeles, CA. Locations within the Delaware River and Bay area include Philadelphia, PA; Islip, NY; Camden, NJ; and Wilmington, DE. Locations within Florida include Pensacola, Panama City, St. Joe, Amelia Island, Jacksonville, Tampa, St. Petersburg, Palmetto, Cape Canaveral, Ft. Pierce, Riviera Beach, Fort Lauderdale, Miami, and Key West.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Transportation workers and individuals, and/or authorized visitors, participating in the Prototype Phase of the Transportation Worker Identification Credential (TWIC) Program who are authorized unescorted entry to secure transportation areas.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system will contain a minimum amount of information during the TWIC Prototype Phase and may include: (1) Individual's name; (2) other demographic data to include: address, phone number, social security number, date of birth, and place of birth; (3) administrative identification codes and unique card serial number; (4) systems identification codes; (5) company/organization or affiliation; (6) issue date; (7) biometric data and digital photograph; (8) access level information; (9) copies of documents that verify address and identity, such as birth certificates, government photo identification, drivers licenses and the like, and (10) expiration date.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 114; 49 U.S.C. 44903(g); 46 U.S.C. 70105.

PURPOSE(S):

In cooperation with transportation facility operators, the records are maintained to evaluate and test certain technologies and business processes in the Prototype Phase of TSA's pilot project to develop a TWIC to improve identity management and access control for transportation workers requiring unescorted access to secure areas of transportation facilities. Additionally, TSA will use certain data elements to support the development and operation of site specific security plans at local transportation facilities. This system is not intended to cover security threat assessments that will be conducted on individuals who seek to obtain a TWIC. Records pertaining to security threat assessments conducted on volunteers of this pilot are maintained in DHS/TSA 002, the Transportation Security Threat Assessment System (T–STAS).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) 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.

(2) To a Federal, State, local, tribal, territorial, foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual as an employee or a contractor, or the issuance of a security clearance or license.

(3) To a Federal, State, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a TSA decision concerning the hiring or retention of an employee, the issuance of a security clearance, license, contract, grant, or other benefit.

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

(6) 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.

(7) To the National Archives and Records Administration or other appropriate Federal agency pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

(8) 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.

(9) To TSA contractors, agents, grantees, experts, consultants, or other like persons 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.

(10) To third parties during the course of an investigation into violations or potential violations of transportation security laws to the extent necessary to obtain information pertinent to the investigation.

(11) To airport operators, aircraft operators, and maritime and land transportation operators and contractors about individuals who are their employees, job applicants, or contractors, or persons to whom they issue identification credentials or grant clearances or access to secured areas in transportation facilities when relevant to such employment, application, contract, the issuance of such credentials or clearances, or access to such secure areas.

(12) To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding individuals who pose or are suspected of posing a risk to transportation or national security.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Paper, bar code, magnetic stripe, optical memory, disk, integrated circuit chip (ICC), and electronic media.

RETRIEVABILITY:

Data records contained within bar codes, magnetic stripe, optical memory stripe, disk, ICC, and/or electronic media may be retrieved by the individuals' name, unique card number, or organization; paper records, where applicable, are retrieved alphabetically by name.

SAFEGUARDS:

Unauthorized personnel are denied physical access to the location where records are stored. For computerized records, safeguards established in accordance with generally acceptable information security guidelines via use of security codes, passwords, Personal Identification Numbers (PINs), etc. Data security and integrity safeguards will be observed during data transmission to the database using strong encryption and digital signing methodologies.

RETENTION AND DISPOSAL:

Record disposition authority for these records is pending at the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director for Compliance, Credentialing Program Office, TSA Headquarters, TSA–19, 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:

TSA obtains information in this system from the individuals who are covered by the system, their employers, or their transportation facility.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Issued in Arlington, Virginia, on September 20, 2004.

Susan T. Tracey,

Chief Administrative Officer.

[FR Doc. 04–21481 Filed 9–23–04; 8:45 am]

BILLING CODE 4910–62–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2004–19160]

Privacy Impact Assessment; Secure Flight Test Phase

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

ACTION: Notice.

SUMMARY: This notice sets forth the Transportation Security Administration's (TSA) Privacy Impact Assessment (PIA) prepared for the testing phase of the Secure Flight program. After a lengthy review of the initial plans for a successor system to Computer Assisted Passenger Prescreening System (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'', which will prescreen airline passengers using information maintained by the Federal Government about individuals known or suspected to be engaged in terrorist activity and certain other information related to passengers' itineraries-specifically, passenger name record (PNR) data. On a limited basis, TSA will also test the use of commercial data to identify instances in which passengers' identifying passenger information is inaccurate or incorrect.

Elsewhere in this edition of the **Federal Register**, TSA is publishing