[Federal Register Volume 75, Number 70 (Tuesday, April 13, 2010)]
[Notices]
[Pages 18867-18871]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2010-8315]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2010-0016]

Privacy Act of 1974; Department of Homeland Security Transportation Security Administration--011, Transportation Security Intelligence Service Operations Files Systems of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice to alter an existing Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to update and reissue a Department of Homeland Security system of records notice titled, Transportation Security Administration--011 Transportation Security Intelligence Service Operations Files previously published on December 10, 2004 to reflect necessary programmatic changes. As a result of the biennial review of this system, modifications are being made to the system of records' categories of individuals, categories of records, routine uses, record source categories, retention and disposal, and notification procedure. The Transportation Security Intelligence Service Operations Filing System contains records on individuals identified in intelligence, counterintelligence, transportation security and information systems security records that relate to the Transportation Security Administration's mission. For example, this system contains information on individuals involved in terrorism or the compromise of classified information.

Portions of this system are exempt under 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5) as reflected in the final rule published in the Federal Register on August 4, 2006.

This updated system will continue to be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before May 13, 2010. This new system will be effective May 13, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS-2010-0016 by one of the following methods:

Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Fax: 703-483-2999.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Peter

[[Page 18868]]

Pietra, Privacy Officer, Transportation Security Administration, TSA-36, 601 South 12th Street, Arlington, VA 20598-6036 or TSAprivacy@dhs.gov. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) Transportation Security Administration (TSA) proposes to update and reissue a DHS/TSA system of records notice titled, DHS/TSA-011, Transportation Security Intelligence Service (TSIS) Operations Files System of Records (69 FR 71828, December 10, 2004).

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. To achieve this mission, TSA is required to develop and adapt its security programs to respond to evolving threats to transportation security. In accordance with the biennial review of this system, the following modifications are being made:

The categories of records section is updated to include biometric records.

DHS/TSA is incorporating four DHS standard routines uses. One routine use will allow release of information to appropriate agencies, entities, and persons when DHS/TSA suspects or has confirmed that the security or confidentiality of an information system of records has been compromised. Another routine use permits the release of information to the media when there exists a legitimate public interest in disclosing information. Release under this routine use will require the approval of the DHS Chief Privacy Officer in consultation with counsel. Another routine use allows the release of information to a court, magistrate, administrative tribunal or opposing counsel or parties where a Federal agency is a party or has an interest in the litigation or administrative proceeding. The fourth routine use allows DHS/TSA to release information to a former employee when it is necessary to consult with the former employee regarding a matter that is within that person's former area of responsibility.

TSA is revising a routine use by adding indirect air carriers and other facility operators as potential recipients of information from these systems when appropriate to address a threat or potential threat to transportation security or national security, or when required for administrative purposes related to the effective and efficient administration of transportation security laws.

TSA is also revising a current routine use by adding indirect air carriers and other facility operators as potential recipients of information 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 when relevant to such employment, application, contract, training or the issuance of such credentials or clearances.

The record source categories are updated to reflect the use of commercial and public record databases and Web sites to obtain information regarding the identity of individuals who attempt to gain access to the sterile areas of the airport and for whom identity needs to be verified or individuals who are being vetted to qualify as Federal flight deck officers. The record source categories to include

Federal, State, local and foreign agencies; formerly only U.S. agencies were included.

For each system of records covered by this notice, the retention and disposal sections are updated to reflect the records retention schedules approved by the National Archives and Records Administration (NARA).

The notification section for each system of records covered by this notice was changed to reflect that inquiries regarding whether the applicable system contains records about an individual should be directed to TSA's Freedom of Information Act (FOIA) Office.

The TSIS Operations Filing System contains records on individuals identified in intelligence, counterintelligence, transportation security and information systems security records that relate to TSA's mission. For example, this system contains information on individuals involved in terrorism or the compromise of classified information. DHS/TSA is revising its system of records to reflect necessary programmatic changes.

Portions of this system are exempt under 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5) as reflected in the final rule published on August 4, 2006 in 71 FR 44223.

Consistent with the Privacy Act, information stored in the TSIS Operations Files System may be shared with other DHS components, as well as appropriate Federal, State, local, Tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a ``system of records.'' A ``system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency recordkeeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/TSA-011 TSIS Operations Files system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM OF RECORDS

DHS/TSA-011

SYSTEM NAME:

Transportation Security Administration 011 Transportation Security Intelligence Service (TSIS) Operations Files.

SECURITY CLASSIFICATION:
Classified, sensitive.

[[Page 18869]]

SYSTEM LOCATION:
Records are maintained at the Transportation Security Administration's Office of the Transportation Security Intelligence Service in Arlington, Virginia and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Individuals identified in intelligence, counterintelligence, transportation security, or information system security reports and supporting materials, including but not limited to individuals involved in matters of intelligence, law enforcement or transportation security, information systems security, the compromise of classified information, or terrorism.

CATEGORIES OF RECORDS IN THE SYSTEM:
Records include biographic and biometric information; intelligence requirements, analysis, and reporting; information systems security analysis and reporting; articles, public-source data, and other published information on individuals and events of interest to TSA; actual or purported compromises of classified intelligence; countermeasures in connection therewith; identification of classified source documents and distribution thereof; records related to transportation security matters (e.g., reports of security-related incidents), and law enforcement records as they pertain to issues involving transportation security.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
49 U.S.C. 114; National Security Act of 1947, as amended, 50 U.S.C. 403-3(d); National Security Agency Act of 1959, Pub. L. 86-36, as amended, 50 U.S.C. 402 Note; E.O. 12333; E.O. 13292 and 12958; E.O. 9397; and National Security Directive 42.

PURPOSE(S):
To maintain records on intelligence, counterintelligence, transportation security, and information systems security matters as they relate to TSA's mission of protecting the nation's transportation systems. To 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:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the privacy act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:
A. To the Department of Justice (DOJ) (including United States attorney Offices) or other Federal agency in anticipation of conducing, or conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:
1. DHS or any component thereof;
2. Any current or former employee of DHS in his/her official capacity, or
3. Any current or former employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or
4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS 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 DHS collected the records.

B. 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 to whom the record pertains.

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

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information;

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, or others performing or working on a contract, service, grant cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, Tribal, local, international, or foreign agency, including law enforcement, or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the United States Department of Transportation, its operating administrations, or the appropriate State or local agency when relevant or necessary to:

1. Ensure safety and security in any mode of transportation;

2. Enforce safety- and security-related regulations and requirements;

3. Assess and distribute intelligence or law enforcement information related to transportation security;

4. Assess and respond to threats to transportation;

5. Oversee the implementation and ensure the adequacy of security measures at airports and other transportation facilities;

6. Plan and coordinate any actions or activities that may affect transportation safety and security or the operations of transportation operators; or

7. The issuance, maintenance, or renewal of a license, certificate, contract, grant, or other benefit.

I. To Federal, State, local, Tribal, territorial, foreign, or international agencies to provide intelligence, counterintelligence, information systems and transportation security information, and other information for the purpose of counterintelligence or antiterrorism activities authorized by U.S. law or Executive Order or for the purpose of enforcing laws that protect national security of the U.S.

J. To U.S. Government agencies regarding compromises of classified information including the document(s) apparently compromised, implications of disclosure of intelligence sources and methods,

investigative data on

[[Page 18870]]

compromises, and statistical and substantive analysis of the data.

K. To any U.S. Government organization in order to facilitate any security, employment, detail, liaison, or contractual decision by any U.S. Government organization, or to facilitate access to any U.S. Government information system.

L. To U.S. agencies involved in the protection of intelligence sources and methods to facilitate such protection and to support intelligence analysis and reporting.

M. 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, contract, grant, or other benefit.

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

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

P. To third parties during the course of or as follow-up to an investigation into violations or potential violations of the law, or an investigation related to the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit, to the extent necessary to obtain information pertinent to the follow-up inquiry or investigation.

Q. To airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers, and other facility operators 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 when relevant to such employment, application, contract, training or the issuance of such credentials or clearances.

R. 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.

S. To airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers, or other facility operators when appropriate to address a threat or potential threat to transportation security, or when required for administrative purposes related to the effective and efficient administration of transportation security laws.

T. To a court, magistrate, or administrative tribunal where a Federal agency is a party to the litigation or administrative proceeding in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings.

U. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

V. To the news media and the public, with the approval of the DHS Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted

invasion of personal privacy or a risk to transportation or national security.

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 maintained on paper, audio and video recordings, and in computer-accessible storage media. Records may also be stored on microfiche and roll microfilm. Records that are sensitive or classified are safeguarded in accordance with agency procedures, and applicable Executive Orders and statutes.

RETRIEVABILITY:
Records may be retrieved by the individual's name, Social Security number, or other assigned personal identifier.

SAFEGUARDS:
Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:
Pursuant to the approved National Archives and Records Administration records retention schedule N1-560-04-12, routine and insignificant case files are destroyed after thirty years; significant case files are retained permanently; watch logs are destroyed after thirty years; watchlists are destroyed 99 years after date of entry or seven years after confirmation of death, whichever is sooner.

SYSTEM MANAGER(S) AND ADDRESS:
Transportation Security Administration, Special Assistant, Office of Intelligence, TSA-10, 601 South 12th Street, Arlington, VA 20598.

NOTIFICATION PROCEDURE:
The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, the Transportation Security Administration will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification and access to any record contained in the system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at https://www.dhs.gov/foia under ``contacts.'' TSA's FOIA Officer is located at: Freedom of Information Act Office, TSA-20, 601 S. 12th Street, 11th Floor, East Tower, Arlington, VA 20598-6020, 1-866-FOIA-TSA or 571-227-2300, Fax: 571-227-1406, E-mail: foia.tsa@dhs.gov. If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0655, Washington, DC 20528.
When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part

[[Page 18871]]

5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

An explanation of why you believe the Department would have information on you,

Identify which component(s) of the Department you believe may have the information about you,

Specify when you believe the records would have been created,

Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURE:

See ``Notification procedure'' above.

CONTESTING RECORD PROCEDURE:

See ``Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from subject individuals; other Federal, State, local and foreign agencies and organizations; hard-copy media, including periodicals, newspapers, and broadcast transcripts, and commercial and public record databases and Web sites; public and classified reporting, intelligence source documents, investigative reports, and correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Portions of this system are exempt under 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5) as reflected in the final rule published on August 4, 2006, in 71 FR 44223.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2010-8315 Filed 4-12-10; 8:45 am]
BILLING CODE 4910-62-P