Federal Register: April 13, 2010 (Volume 75, Number 70)]
[Notices]
[Page 18860-18863]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr13ap10-71]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2010-0017]

Privacy Act of 1974, Department of Homeland Security Transportation Security Administration--013 Federal Flight Deck Officer Record System

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 an existing Department of Homeland Security system of records notice titled, Transportation Security Administration--013 Federal Flight Deck Officer Record System, previously published on August 18, 2003. The Federal Flight Deck Officer Record System contains records necessary for assessment, acceptance, training, participation, and recertification of deputized pilots of commercial air carriers who participate in the Flight Deck Officer Program designed to defend aircraft flight decks against acts of criminal violence or air piracy.

As a result of the biennial review of this system, modifications are being made to the system of records' routine uses, record sources, retention and disposal, notification procedures, and system manager and address.

Portions of this system are exempt under 5 U.S.C. 552a(k)(1), (k)(2) and (k)(6) as reflected in the final rule published in the Federal Register on June 25, 2004.

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. The system will be effective May 13, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS-2010-0017 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 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-013 Federal Flight Deck Officer Record System (FDORS), previously published on August 18, 2003 (68 FR 49496).

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:

DHS/TSA is updating the system of records to incorporate five Department of Homeland Security (DHS) standard routines uses. One routine use will allow the 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. The third 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. The fifth routine use allows DHS/TSA to release information to appropriate entities where it would assist in the enforcement of civil or criminal laws.

DHS/TSA is revising a routine use currently in 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.

DHS/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.

Finally, DHS/TSA has removed as a routine use the sharing of information with the Attorney General of the United States concerning violations of the Brady Handgun Violence Prevention Act as it is duplicative.

The record source categories are being 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 retention and disposal section is updated to reflect the records retention schedules approved by the National Archives and Records Administration (NARA).

The notification section 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 system manager and address were revised to reflect the current system manager.

[[Page 18861]]

FFDORS contains records necessary for assessment, acceptance, training, participation, and recertification of deputized pilots of commercial air carriers who participate in the Flight Deck Officer Program designed to defend aircraft flight decks against acts of criminal violence or air piracy.

As a result of the biennial review of this system, modifications are being made to the system of records' routine uses, record sources, retention and disposal, notification procedures, and system manager and address.

Portions of this system are exempt under 5 U.S.C. 552a(k)(1), (k)(2) and (k)(6) as reflected in the final rule published on June 25, 2004, 69 FR 35536.

Consistent with the Privacy Act, information shared in the Federal Flight Deck Officer Records 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

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 individual's 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 record keeping practices transparent, to notify individuals regarding the uses to which their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the Transportation Security Administration 013 Federal Flight Deck Officer Record System 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 013

System name:

Transportation Security Administration 013 Federal Flight Deck Officer Record System (FFDORS).

Security classification:

Classified, sensitive.

System location:

Federal Flight Deck Officer (FFDO) Program Records are maintained at the offices of the Transportation Security Administration (TSA) Headquarters in Reston, Virginia.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

1. All individuals who volunteer to participate in the FFDO program,

2. FFDO program participants, i.e., those volunteers who are accepted into the FFDO training program and deputized as FFDOs, and

3. former FFDO program participants.

Categories of records in the system:

This system includes all records required in connection with an individual's voluntary participation in the program, including records associated with FFDO application, selection, training, participation, retention and requalification. FFDORS includes records about individuals who applied but were not accepted into the program. Such records may include, but are not limited to the following:

(a) Volunteer forms prepared by applicants for program participation containing such information as work history, education, military service, certificates of specialized training, awards and honors;

(b) Copies of correspondence between the applicant and TSA, and between TSA and other agencies, applicant places of employment, and educational institutions, for the purposes of verifying information

provided to TSA by the applicant;
(c) The FD-258 Fingerprint card, investigative summaries, and compilations of criminal history record checks, to include administrative records and correspondence incidental to the background investigation process, obtained from various law enforcement authorities;
(d) Results of written cognitive and noncognitive assessments and information regarding how the volunteer form was rated, prepared by TSA employees or contract psychologists;
(e) Records regarding the TSA's final decision to accept or reject volunteers for the FFDO program for suitability or medical reasons, including records prepared by TSA employees, and responses to and results of approved psychological assessments or similar tests administered by TSA;
(f) Results of telephonic or in-person interviews with program volunteers, including summary recommendations regarding the individual's participation in the program, prepared by TSA employees;
(g) Records prepared by TSA employees related to the selection or rejection of volunteer applicants (to include records generated as a result of any administrative appeal of TSA's determination to reject an applicant), and records related to recertification and decertification;
(h) Records prepared by TSA employees related to training, including academic and firearms performance; and
(i) Records prepared by TSA employees related to requalification and deputation renewal.

Authority for maintenance of the system:
49 U.S.C. 114, 44921.

Purpose(s):
The purpose of this system is to maintain records necessary for the assessment and acceptance of volunteers, and the training, participation and recertification of deputized volunteer pilots of air carriers providing commercial air transportation as federal law enforcement to defend the flight decks of aircraft of such air carriers against acts of criminal violence or air piracy.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:
A. To the Department of Justice (DOJ) (including United States Attorney Offices) or other federal agency in

anticipation of, 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;
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 government 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. The Department 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) or harm to the individual that rely upon the compromised information; and

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, and 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 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.

J. 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.

K. 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.

L. 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.

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

N. To third parties to the extent necessary to obtain information pertinent to the individual's fitness and qualifications for the FFDO program.

O. To airport operators, aircraft operators, and 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.

P. To the DOJ in review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which DHS/TSA exercises jurisdiction.

Q. 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-relate 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.

R. 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.

S. To the appropriate Federal, State, local, tribal, territorial, foreign, or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, order, license, or treaty, where DHS/TSA determines that the information would assist in the enforcement of a civil or criminal laws.

T. To the news media and the public, with the approval of the DHS Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, 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 in this system may be maintained on paper 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:

Information can be retrieved by name, address, social security, and account number or other assigned tracking 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. These safeguards include restricting access to authorized personnel who have a need-to-know; using locks, alarm devices, and passwords; and encrypting data communications. TSA file areas are locked after normal duty hours and security personnel protect the facilities from the outside.

Retention and disposal:

Records associated with the assessment of FFDO's will be destroyed one year after TSA is notified that access based on security threat assessment is no longer valid; where an individual was a possible match to a watchlist, records will be destroyed seven years after completion of the security threat assessment or one year after being notified that access based on the security threat assessment is no longer valid, whichever is longer; and where the individual is an actual match to a watchlist records will be destroyed 99 years after the security threat assessment or seven years after TSA is notified the individual is deceased, whichever is shorter.

System managers and address:

Transportation Security Administration, Office of Law Enforcement/ Federal Air Marshal Service. 1900 Oracle Way, Suite 500, Reston, VA 20190.

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, TSA 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 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 procedures:

See ``Notification procedure'' above.

Contesting record procedures:

See ``Notification procedure'' above.

Record source categories:

Information maintained in this system is primarily obtained from the FFDO volunteer form or derived from information the applicant supplied, reports from medical personnel on physical and psychological results of examinations, training records, and law enforcement and intelligence agency record systems, commercial and public databases and Web sites and individuals interviewed as part of the background investigation.

Exemptions claimed for the system:

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

(k)(2) and (k)(6) as reflected in the final rule published on June 25, 2004.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2010-8317 Filed 4-12-10; 8:45 am]
BILLING CODE 4910-62-P