[Federal Register Volume 75, Number 35 (Tuesday, February 23, 2010)]
[Notices]
[Pages 8088-8092]
From the Federal Register Online via the Government Publishing Office
[www.gpo.gov]
[FR Doc No: 2010-3362]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2009-0041]

Privacy Act of 1974; Department of Homeland Security/ALL--023 Personnel Security Management System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue Department of Homeland Security/ALL--023 Personnel Security Management System of Records to include record systems within the Federal Protective Service and records of federal, state, local and foreign law enforcement personnel who apply for and/or are granted authority to enforce federal laws on behalf of the Department. Categories of individuals, categories of records, purpose, and routine uses of this system have been reviewed and updated to reflect the personnel security management record systems of the Department, including the Federal Protective Service. The activities performed by the Department's personnel security program often overlap with other security-related activities such as access control and investigatory records. Accordingly, data within each of the categories of individuals, categories of records, purpose and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose.

Further, this system of records is separate from Department of Homeland Security/ALL 026--Personal Identity Verification Management System of Records, June 25, 2009, which supports the administration of the Homeland Security Presidential Directive--12 program, directing the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems while enhancing security, increasing efficiency, reducing identity fraud, and protecting personal privacy.

There will be no change to the Privacy Act exemptions currently in place for this system of records and therefore remain in effect. This updated system will continue to be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before March 25, 2010. This updated system will be effective March 25, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS-2009-0041 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 and may be read at 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 and privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Homeland Security (DHS) and its components and offices rely on DHS/ALL--023 Personnel Security Management System of Records (74 FR 3084, January 16, 2009) for the collection and maintenance of records that pertain to personnel security management.

DHS is updating and reissuing this Department-wide system of records under the Privacy Act (5 U.S.C. 552a), for DHS personnel security management records, to include records systems within the Federal Protective Service (FPS) and records of federal, state, local, and foreign law enforcement personnel

[[Page 8089]]

who apply for and/or are granted authority to enforce federal laws on behalf of DHS. The DHS/ALL--023 Personnel Security Management System of Records is the baseline system for personnel security activities, as led by the DHS Office of the Chief Security Officer, for the Department. This will ensure that all DHS components follow the same privacy rules for collecting and handling personnel security management records.

The purpose of this system is to maintain processing records of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. Also, records may be used by the Department for adverse personnel actions such as removal from sensitive duties, removal from employment, and denial to a restricted or sensitive area, and revocation of security clearance. The system also assists in capturing background investigations and adjudications; directing the clearance process for granting, suspending, revoking and denying access to classified information; directing the clearance process for granting, suspending, revoking and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of DHS; managing state, local, and

private-sector clearance programs and contractor suitability programs; determining eligibility for unescorted access to DHS facilities or information technology systems; and other activities relating to personnel security management responsibilities at DHS. The Department's authority for this collection is primarily 5 U.S.C. 301; 44 U.S.C. 3101; 8 U.S.C. 1357(g); 19 U.S.C. 1401(i); Executive Order (EO) 9397; EO 10450; EO 12968; 5 CFR part 731; 5 CFR part 732; 5 CFR part 736; 32 CFR part 147; and DCID 6/4. This system will collect individuals' personal information to support the Department's efforts related to their personnel security activity. Efforts have been made to safeguard records in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize 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. The routine uses posted are unchanged from the previous publishing and consistent with the purpose for collection. This system of records is collecting information under the Paperwork Reduction Act using the following forms: (1.) Questionnaire for Non-Sensitive Positions--SF-85--OMB No. 3206-0005; (2.) Questionnaire for Public Trust Position--SF-85P--OMB No. 3206-0191; (3.) Supplemental Questionnaire for Selected Positions--SF-85P-S OMB No. 3206-0191; (4.) Questionnaire for National Security Positions--SF-86--OMB No. 3206-0005; and (5.) Continuation Sheet for Questionnaires--SF-86A--OMB No. 3206-0005. Further reviews are being conducted to determine if the system of records collects other information under the Paperwork Reduction Act. Categories of individuals, categories of records, the purpose, and routine uses of this system have been reviewed and updated to reflect the personnel security management record systems of the Department, including the FPS. The Privacy Office has updated the categories of individuals covered by the system to include DHS-covered individuals, such as federal employees, applicants, excepted service federal employees, contractor employees, retired employees, past employees providing support to DHS and who require unescorted access to DHS-secured facilities, and federal, state, local, and foreign law enforcement personnel who apply for or are granted authority to enforce federal laws on behalf of DHS. The categories of records have been updated to include facial photographs and criminal background investigations. The purpose has been revised to reflect that the system assists in directing the clearance process for granting, suspending, revoking and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of DHS and eligibility for unescorted access to DHS secured facilities. An existing routine use (Routine Use H) was modified to permit the sharing of information from this system of records with agencies where it is relevant and necessary to the agencies' decision concerning the delegation or designation of authority. Lastly, a new routine use was added to permit sharing of information with the news media and the public, with the approval of the 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 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.

Privacy Impact Assessments (PIAs) have been conducted and are on file for the (1.) Personnel Security Activities Management System; (2.) Integrated Security Management System; (3.) DHSAccessGate System; (4.) Automated Continuing Evaluation System (ACES) Pilot; (5.) Personal Identity Verification System; (6.) Federal Protective Service Information Support Tracking System (FISTS) Contract Suitability Module; and (7.) Federal Protective Service Dispatch Incident Records Management Systems along with other related component specific PIAs and can be found at http://www.dhs.gov/privacy.

Consistent with DHS's information sharing mission, information stored within the DHS/ALL--023 Personnel Security Management System of Records 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.

The Office of the Chief Security Officer is implementing a new web-based personnel and information security application, Integrated Security Management System (ISMS). ISMS has replaced many of the existing case management systems currently in use at the Department's Headquarters, U.S. Customs and Border Protection (CBP), the Federal Law Enforcement Training Center (FLETC), and the Federal Emergency Management Agency (FEMA). ISMS will replace the existing case management systems currently in use at the U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and the U.S. Coast Guard (USCG) in the near future.

There will be no change to the Privacy Act exemptions currently in place for this system of records and therefore remain in effect. This updated system will continue to be included in DHS's inventory of record systems.

[[Page 8090]]

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 an 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 from which information is stored and retrieved by the name of the individual or by some identifying number such as property address, mailing address, or symbol assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. DHS extends administrative Privacy Act protections to all individuals where information is maintained on both U.S. citizens, lawful permanent residents, and visitors. Individuals may request 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 of their records, and to assist individuals to more easily find such files within the agency. Below is a description of DHS/ALL--023 Personnel Security Management System of Records.

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

System of Records

DHS/ALL-023

System name:

Department of Homeland Security (DHS)/ALL--023 Personnel Security Management System of Records.

Security classification:

Unclassified, sensitive, for official use only, and classified.

System location:

Records are maintained at several DHS Headquarters locations and component offices in Washington, DC and field locations; and the Department of Treasury (DTR), Bureau of Public Debt for Office of Inspector General employees and applicants. For background investigations adjudicated by the Office of Personnel Management (OPM), OPM may retain copies of those files pursuant to their records retention schedules.

Categories of individuals covered by the system:

Categories of individuals covered by this system include federal employees, applicants, excepted service federal employees, contractor employees, retired employees, and past employees providing support to DHS who require: (1.) Unescorted access to DHS-owned facilities, DHS-controlled facilities, DHS-secured facilities, or commercial facilities operating on behalf of DHS; (2.) access to DHS information technology (IT) systems and the systems' data; or (3.) access to national security information including classified information.

Also covered are: (1.) State and local government personnel and private-sector individuals who serve on an advisory committee or board sponsored by DHS; (2.) federal, state, local, and foreign law enforcement personnel who apply for or are granted authority to enforce federal laws on behalf of DHS; and (3.) individuals, including state and local government personnel and private-sector individuals, who are authorized by DHS to access Departmental facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information.

Categories of records in the system:

Categories of records in the system include:

- Individual's name;
- Date and place of birth;
- Social security number;
- Citizenship;
- Access Control Pass or Credential number;
- Facial photograph;
- Records relating to the management and operation of DHS personnel security program, including but not limited to:

[cir] Completed standard form questionnaires issued by the Office

of Personnel Management;
[cir] Originals or copies of background investigative reports;
[cir] Supporting documentation related to the background investigations and adjudications including criminal background, medical and financial data;
[cir] Information related to congressional inquiry; and
[cir] Other information relating to an individual's eligibility for access to classified or sensitive information.

Records relating to management and operation of DHS programs to safeguard classified and sensitive but unclassified information, including but not limited to:
[cir] Document control registries;
[cir] Courier authorization requests;
[cir] Non-disclosure agreements;
[cir] Records of security violations;
[cir] Records of document transmittals; and
[cir] Requests for secure storage and communications equipment.

Records relating to the management and operation of DHS special security programs, including but not limited to:
[cir] Requests for access to sensitive compartmented information (SCI);
[cir] Contact with foreign officials and foreign travel registries; and
[cir] Briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations.

Records relating to the management and operation of the DHS security program, including but not limited to:
[cir] Inquiries relating to suspected security violation(s);
[cir] Recommended remedial actions for possible security violation(s);
[cir] Reports of investigation regarding security violations;
[cir] Statements of individuals;
[cir] Affidavits;
[cir] Correspondence;
[cir] Documentation pertaining to investigative or analytical efforts by DHS Security program personnel to identify threats to DHS personnel, property, facilities, and information; and
[cir] Intelligence reports and database results relating to DHS personnel, applicants, or candidates for DHS employment or access to DHS facilities or information.

Authority for maintenance of the system:
5 U.S.C. 301; 44 U.S.C. 3101; 8 U.S.C. 1357(g); 19 U.S.C. 1401(i); Executive Order (EO) 9397; EO 10450; EO 12968; 5 CFR part 731; 5 CFR part 732; 5 CFR part 736; 32 CFR part 147; and DCID 6/4.

Purpose(s):
The purpose of this system is to collect and maintain records of processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. Also, records may be used by the Department for adverse

personnel actions such as removal from sensitive duties, removal from employment, denial to a restricted or sensitive area, and/or revocation of security clearance. The system also assists in capturing background investigations and adjudications; directing the clearance process for granting, suspending, revoking and denying access to classified information; directing the clearance process for granting, suspending, revoking and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of DHS; managing state, local and private-sector clearance programs and contractor suitability programs; determining eligibility for unescorted access to DHS owned, occupied or secured facilities or information technology systems; and/or other activities relating to personnel security management responsibilities at DHS.

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 of 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 (including United States Attorney Offices) or other federal agency 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 employee of DHS in his/her official capacity;

3. Any 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 written 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 who relies 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 law enforcement agency 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 an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To an individual's prospective or current employer to the extent necessary to determine employment eligibility.

J. To a court, magistrate, or administrative tribunal 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 or pursuant to the order of a court of competent jurisdiction in response to a subpoena from a court of competent jurisdiction.

K. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

L. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

M. To the news media and the public, with the approval of the 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.

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 are stored electronically or on paper in secure

facilities in a locked drawer behind a locked door. The records are stored on servers, magnetic disc, tape, digital media, and CD-ROM.

Retrievability:
Records may be retrieved by individual's name, date of birth, social security number, if applicable, or other unique individual identifier such as access control pass or credential number.

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 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 GRS 18, Item 21 through 25, records relating to alleged security violations are destroyed two years after completion of final action or when no longer needed, whichever is sooner; records relating to alleged violations of a sufficient serious nature that are referred for prosecutive determinations are destroyed five years after the close of the case; personnel security clearance files are destroyed upon notification of death or not later than five years after separation or transfer of employee or no later than five years after contract relationship expires, whichever is applicable.

System Manager and address:
For Headquarters components of DHS: Chief, Personnel Security Division (202-447-5010), Office of Security, Department of Homeland Security, Washington, DC 20528. For components of DHS, the System Manager can be found at http://www.dhs.gov/foia under ``contacts.''

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, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this 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

http://www.dhs.gov/foia under ``contacts.'' 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 and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0550, 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 Chief Privacy Officer and Chief Freedom of Information Act Officer, 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; and
- 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:

Records are generated from sources contacted during personnel and background investigations.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(1), (k)(2), (k)(3), and (k)(5) of the Privacy Act.

Dated: February 1, 2010.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010-3362 Filed 2-22-10; 8:45 am]
BILLING CODE 9110-9B-P