[Federal Register Volume 75, Number 22 (Wednesday, February 3, 2010)]
[Notices]
[Pages 5609-5614]
From the Federal Register Online via the Government Publishing Office
[www.gpo.gov]
[FR Doc No: 2010-2206]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2009-0042]

Privacy Act of 1974; Department of Homeland Security/ALL--024 Facility and Perimeter Access Control and Visitor 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--024 Facility and Perimeter Access Control and Visitor Management System of Records to include record systems within the Federal Protective Service. Categories of individuals, categories of records, purpose and routine uses of this system have been reviewed and updated to better reflect the Department's, including the Federal Protective Service's, facility and perimeter access control and visitor management record system. The activities performed by the Department's facility and perimeter access control and visitor management systems often overlap with other security-related activities. Accordingly, data within each of the categories of individuals, categories of records, 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.

Records within this system apply only to perimeters and facilities where access is controlled by the Department of Homeland Security or its components, including the Federal Protective Service, and its contract guards.

Exclusion is made to perimeters and facilities secured by the U.S. Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. Records pertaining to perimeters and facilities secured by the

U.S. Secret Service, other than those records subject to the Presidential Records Act, are covered under Department of Homeland Security/U.S. Secret Service--004 Protection Information System of Records, December 19, 2008.

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

DATES: Written comments must be submitted on or before March 5, 2010. This updated system will be effective March 5, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS-2009-0042 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--024 Facility and Perimeter Access Control and Visitor Management System of Records (74 FR 3081, January 16, 2009) for the collection and maintenance of records that pertain to facility and perimeter access control and visitor management.

DHS is updating and reissuing this Department-wide system of records under the Privacy Act (5 U.S.C. 552a) for DHS facility and perimeter access control and visitor management records, to include records systems within the Federal Protective Service (FPS). DHS/ALL--024 Facility and Perimeter Access Control and Visitor Management System of Records is the baseline system for facility and perimeter access control and visitor management, as led by the Office of the Chief Security Officer. This will ensure that all components of DHS follow the same privacy rules for collecting and handling access control and visitor management records.

The purpose of this system is to collect and maintain records related to the Department's facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management. The

Department's authority for this collection is primarily 5 U.S.C. 301; the Homeland Security Act, codified in Title 6 of the U.S. Code; 44 U.S.C. 3101; Executive Order (EO) 9397; EO 12968; and Federal Property Regulations, issued July 2002. This system will collect individuals' personal information to support the Department's efforts related to protecting DHS facilities and operating the visitor management program. 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 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. The routine uses posted are unchanged from the previous publishing and consistent with the purpose for collection. A review of this system is being conducted to determine if the system of records collects 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 better reflect the Department's, and FPS's, facility and perimeter access control and visitor management records system. Specifically, the Department has: Updated categories of individuals to include any employee, contractor, consultant, intern, fellow, or other person with regular access and an access control pass which grants unescorted access to a DHS facility or other federal facility which DHS or its components provide access control, including the FPS and its contract guards, and those needing access to information technology systems, and any visitor to a facility for which DHS or its components provide access control and violators and those accused of security violations of access or perimeter control and those related to incidents and offenses in and around these facilities, and individuals, including state and local government personnel and private-sector individuals, who are authorized by DHS to access DHS facilities, and other federal facilities where DHS controls access through its components, including the FPS and its contract guards; updated categories of records to include information pertaining to incidents and offenses; updated routine uses to include disclosing information outside DHS to an appropriate federal, state, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence, but only when the disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure, and disclosing information to an appropriate federal, state, local, tribal, or foreign government agency, international organization, or private organization where the President or the Secretary of Homeland Security has declared an event to be a National Special Security Event; and record source categories has been updated to include records which are obtained from individuals seeking employment or access to facilities for which DHS and its components provide security and from individuals involved in incidents and offenses that take place in or around those facilities.

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; (7) Federal Protective Service Dispatch Incident Records Management Systems; and (8) Livewave CCTV System 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 in the DHS/ALL--024 Facility and Perimeter Access Control and Visitor

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.

Records within this system apply only to perimeters and facilities where access is controlled by DHS or its components, including the FPS, and its contract guards.

Exclusion is made to perimeters and facilities secured by the U.S. Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. Records pertaining to perimeters and facilities secured by the U.S. Secret Service, other than those records subject to the Presidential Records Act, are covered under Department of Homeland Security/U.S. Secret Service--004 Protection Information System of Records (73 FR 77733, December 19, 2008).

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

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 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 5.21.

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--024 Facility and Perimeter Access Control and Visitor 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-024

System name:

Department of Homeland Security (DHS)/ALL--024 Facility and Perimeter Access Control and Visitor 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 in component offices in both Washington, DC and field locations.

Categories of individuals covered by the system:

Categories of individuals covered by this system include: (1) Any employee, contractor, consultant, intern, fellow, or others with regular access and an access control pass which grants unescorted access to a DHS facility or other federal facility which DHS or its components provide access control, including the FPS and its contract guards, and those needing access to information technology systems, and any visitor to a facility for which DHS or its components provide access control; (2) violators and those accused of security violations of access or perimeter control and those related to incidents and offenses in and around these facilities; (3) applicants for employment, contractors, or those needing unescorted access to these facilities or information technology systems; (4) state and local government personnel and private-sector individuals who serve on an advisory committee and board sponsored by DHS; (5) individuals, including state and local government personnel and private-sector individuals, who are authorized by DHS to access DHS facilities, and other federal facilities where DHS controls access through its components, including the FPS and its contract guards, including classified facilities, communications security equipment, and information technology systems that process national or homeland security classified information.

Categories of records in the system:

Categories of records in the system include:

- Individual's full name;
- Date and place of birth;
- Social security number;

Note: For access to the Nebraska Avenue Complex, DHS employees, including component employees and contractors, are not required to provide date of birth or social security number to enter the Nebraska Avenue Complex if they provide a HSPD-12 badge, component badge, credential, or commission book. Component employees and contractors will also provide name, component, and Nebraska Avenue Complex point of contact name and phone number. Headquarters employees and contractors can also provide a drivers license as

identification to be confirmed within the system of records as a DHS Headquarters employee. If a component employee or contractor does not have a DHS or component-issued credential at the point of entry, the individual will be processed into the Nebraska Avenue Complex as a regular visitor requiring a full name, date of birth, and social security number.

Organization's name;
Citizenship;
Country of origin, if applicable;
Telephone number;
Physical descriptions;
Biometric information;
Photograph;
Visitor badge number, if applicable;
Date and time of entry and departure;
Drivers license and other form of identification information;
License plate number and state of issuance;
Make and model of vehicle;
Reports, files, records received from other federal agencies;
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 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] Information pertaining to incidents and offenses;
[cir] Statements of individuals;
[cir] Affidavits; and
[cir] Correspondence.

Records relating to the management and operation of the facility and perimeter access control and visitor management system including but not limited to:

[cir] Facility and perimeter access registries;
[cir] Courier cards;
[cir] Access control card requests; and
[cir] Specific information from standard DHS forms used to conduct criminal history record checks; and
[cir] Closed circuit television (CCTV) systems and recordings.

Authority for maintenance of the system:

5 U.S.C. 301; the Homeland Security Act, codified in Title 6 of the U.S. Code; 44 U.S.C. 3101; and Executive Order (EO) 9397; EO 12968; and

Federal Property Regulations, issued July 2002.

Purpose(s):

The purpose of this system is to collect and maintain records associated with DHS facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management.

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 or contract provider, 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, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee or contractor, the issuance of a security clearance, the reporting of an investigation of an employee or contractor, the letting of a contract, or the issuance of a license, grant or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. 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.

J. To an appropriate federal, state, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence, but only when the disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure, and;

K. To an appropriate federal, state, local, tribal, or foreign government agency, international organization, or private organization where the President or the Secretary of Department of Homeland Security has declared an event to be a National Special Security Event, 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, 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 or other benefit, but only when disclosure is appropriate to the proper performance of the official duties of the person making the request.

L. 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 name, date of birth, and social security number, or other personal identifier listed above in ``Category of Records in the System,'' if applicable.

Note: For access to DHS Headquarters, all employees, including component employees and contractors, are not required to provide date of birth and social security number to enter DHS Headquarters facilities. If they do not have their credential at the point of entry, they are required to log their name and title, component, data and time, ID of employee, and point of contact.

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 22a, 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.
Pursuant to GRS 18, Item 6, requests and authorizations for individuals to have access to classified files are destroyed two years after authorization expires.
Pursuant to GRS 11, Item 4a, identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors' passes, and other identification credentials are destroyed three months after return to issuing office.
Pursuant to GRS 18, Item 17, registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers for areas under maximum security are destroyed five years after final entry or five years after date of document, as appropriate.

Other documents pursuant to GRS 18, Item 17b, are destroyed two years after final entry or two years after date of document, as appropriate.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding, the records will be retained until final disposition of the investigation or proceeding.

System Manager and address:

For Headquarters components of DHS: Chief, Physical 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 obtained from individuals seeking employment or access to facilities for which DHS and its components provide security and from individuals involved in incidents and offenses that take place in or around those facilities.

[[Page 5614]]

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), and (k)(5) of the Privacy Act.

Dated: January 25, 2010.
Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2010-2206 Filed 2-2-10; 8:45 am]
BILLING CODE 9110-9B-P