[Federal Register: September 12, 2006 (Volume 71, Number 176)]
[Notices]
[Page 53697-53700]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr12se06-69]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket Number DHS-2006-0047]

Privacy Act; Systems of Records

AGENCY: Office of Security, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security, Office of Security, proposes to add a new system of records to the Department's inventory, entitled the ``Personal Identity Verification Management System.'' This system will support the administration of the HSPD-12 program that directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This system will enhance security, increase efficiency, reduce identify fraud, and protect personal privacy.

DATES: The established system of records will be effective October 12,

[[Page 53698]]

2006, unless comments are received that result in a contrary determination.

ADDRESSES: You may submit comments identified by docket number DHS-2006-0047 by one of the following methods:

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

Fax: (202) 401-4514 (not a toll-free number).

Mail: Cynthia Sjoberg, Office, DHS HSPD-12 Program Manager, Office of Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528; Hugo Teufel III, Chief Privacy Officer, 601 S. 12th Street, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Cynthia Sjoberg, DHS HSPD-12 Program Manager, Office of Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528 by telephone (202) 772-5096 or facsimile (202) 401-4514; Hugo Teufel III, Chief Privacy Officer, 601 S. 12th Street, Arlington, VA 22202 by telephone (571) 227-3813 or facsimile (571) 227-

4171.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security (DHS), Office of Security is publishing a Privacy Act system of records notice to cover its collection, use and maintenance of records relating to its role in the collection and management of personally identifiable information for the purpose of issuing credentials (ID badges) to meet the requirements of the Homeland Security Presidential Directive-12 (HSPD-12) and in furtherance of the Office of Security's mission for the Department. Until now, pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Sec. 1512, 116 Stat. 2310 (Nov. 25, 2002) (6 U.S.C. 552), the Office of Security has been relying on legacy Privacy Act systems for this purpose.

DHS established the Office of Security to protect and safeguard the Department's personnel, property, facilities, and information. The Office of Security develops, coordinates, implements, and oversees the Department's security policies, programs, and standards; delivers security training and education to DHS personnel; and provides security support to DHS components when necessary. In addition, the Office of Security coordinates and collaborates with the Intelligence Community on security issues and the protection of information. The Office of Security works to integrate security into every aspect of the Department's operations.

The Office of Security is divided into seven divisions, as follows, and in order of relevance to this notice:

Security Operations: This division implements and maintains the Department's badging and credentialing programs and ensures that the Department is in full compliance with all applicable laws. It is within this Division and area of responsibility that the Office of Security is giving notice of its intent to create the Personal Identity Verification Management System (PIVMS) pursuant to HSPD-12;

Personnel Security: background investigations, adjudications, and security clearances for DHS employees, as well as for State and local government personnel and private-sector partners;

Administrative Security: the protection of classified and sensitive but unclassified information;

Physical Security: security surveys, vulnerability assessments, and access control for DHS facilities;

Special Security Programs: Sensitive Compartmented Information (SCI) and Special Access Programs;

Internal Security and Investigations: protection against espionage, foreign intelligence service elicitation activities, and terrorist collection efforts directed against the Department; investigations of crimes against the Department's personnel and property;

Training and Operations Security: integrated security training policy and programs.

The PIVMS records will cover all DHS employees, contractors and their employees, consultants, volunteers engaged by DHS who require long-term access to federal buildings and emergency ``first responders'' who work in federally controlled facilities. The personal information to be collected will consist of data elements necessary to identify the individual and to perform background or other investigations concerning the individual. The PIVMS will collect several data elements from the PIV card applicant, including: date of birth, Social Security Number, organizational and employee

affiliations, fingerprints, digital color photograph, digital signature and phone number(s) as well additional verification information. The Office of Security has designed this system to align closely with their current business practices.

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 personally identifiable information. The Privacy Act applies to information that a Federal agency maintains in a ``system of records.'' A ``system of records'' is a group of any records under the control of an agency from which the agency retrieves information by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Office of Security Personal Identity Verification Management System is such a system of records.

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 personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the Personal Identity Verification Management System.

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

DHS-OS-2006-047

System name:

Personal Identity Verification Management System (PIVMS).

Security Classification:

Sensitive but unclassified.

System Location:

Data covered by this system are maintained at the following location: DHS Data Center, Ashburn, VA.

Categories of Individuals Covered By the System:

The PIVMS records will cover all DHS employees, contractors and their employees, consultants, volunteers engaged by DHS who require long-term access to federal buildings and emergency ``first responders'' who work in federally controlled facilities. Individuals who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security.

The system does not apply to occasional visitors or short-term guests to whom DHS will issue temporary identification and credentials.

Categories of Records in the System:

Records maintained on individuals issued a PIV credential by DHS include the following data fields: full name; Social Security number; date of birth; current address; digital signature; digital color photograph; fingerprints; biometric identifiers (two fingerprints);

organization/office of assignment; employee affiliation; telephone

number(s); copies of identity source documents; signed SF 85 or equivalent; PIV card issue and expiration dates; PIV request form; PIV registrar approval digital signature; PIV card serial number; emergency responder designation; computer system user name; user access and permission rights, authentication certificates; digital signature information.

Authority for Maintenance of the System:

5 U.S.C. 301; Federal Information Security Act (Pub.L. 104-106, Sec. 5113); E-Government Act (Pub.L. 104-347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); and the Government Paperwork Elimination Act (Pub.L. 105-277, 44 U.S.C. 3504); Homeland Security Presidential Directive-12 (HSPD-12); Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, Section 3001 (50 U.S.C. 435b) and the Homeland Security Act of 2002, P.L. 107-296, as amended.

Purpose(s):

The primary purposes of the system are: (a) To ensure the safety and security of DHS facilities, systems, or information, and our occupants and users; (b) To verify that all persons entering Federal facilities, using Federal information resources, are authorized to do so; (c) to track and control PIV cards issued to persons entering and exiting the DHS facilities or using DHS systems.

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. Section 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) when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

B. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

C. Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program

statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

D. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

E. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

F. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

G. To a Federal State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.

H. To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

I. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

J. To notify another Federal agency when, or verify whether, a PIV card is no longer valid.

K. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards.

L. To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

Disclosure to consumer reporting agencies:

Privacy Act information may be reported to consumer reporting agencies pursuant to 5 U.S.C. 552a(b)(12).

Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records in the System:

Storage:

DHS Headquarters in the Offices of Security and Human Capital and at the DHS Data Center in Ashburn, VA Records maintain and store the records in electronic media and paper files.

Retrievability:
Records may be retrieved by name of the individual, Social Security number

[[Page 53700]]

and/or by any other unique individual identifier.

Safeguards:
The Office of Security protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a ``need to know'' basis, utilization of SmartCard access, and locks on doors and approved storage containers. DHS buildings have security guards and secured doors. DHS monitors all entrances through electronic surveillance equipment. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. DHS encrypts data storage and transfer. DHS maintains an audit trail and engages in random periodic reviews to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.

Retention and Disposal:
This is a new program and the Records Management Office (RMO) has not finalized its retention policy. The DHS RMO will develop a records retention schedule for approval by the NARA pertaining to this program. Once NARA has approved the records retention schedule, DHS will amend this document to include the retention period for the records.

System Manager and address:
DHS HSPD-12 Program Manager, Office of Security, U.S. Department of Homeland Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528.

Notification procedure:
A request for access to records in this system may be made by writing to the System Manager, or the Director of Departmental Disclosure, in conformance with 6 CFR part 5, which provides the rules for requesting access to records maintained by the Department of Homeland Security.

Record access procedures:
Same as Notification Procedure above.

Contesting record procedures:
Same as Notification Procedure above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other Federal agencies; contract employer; former employer.

Exemptions claimed for the system:
None.

Dated: September 1, 2006.
Hugo Teufel III,
Chief Privacy Officer.
[FR Doc. E6-15044 Filed 9-11-06; 8:45 am]

BILLING CODE 4410-10-P