FR Doc E6-15901
[Federal Register: September 28, 2006 (Volume 71, Number 188)]
[Notices]
[Page 56983-56986]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr28se06-65]

==========

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Proposed Privacy Act System of Records

AGENCY: General Services Administration.

ACTION: Notice of Privacy Act system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the General Services Administration (GSA) proposes to establish a new system of records titled the Federal Personal Identity Verification Identity Management System (PIV IDMS) (GSA-GOVT-7). This system will support the implementation of Homeland Security Presidential Directive 12 (HSPD-12) by providing a GSA managed shared infrastructure and services for participating Federal agencies. HSPD-12 requires 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 identity fraud, and protect personal privacy.

DATES: The established system of records will be effective 30 days after publication of this Notice.

ADDRESSES: Comments may be submitted to the Director, HSPD-12 Managed Service Office, Federal Acquisition Service, General Services Administration, Suite 911, 2011 Crystal Drive, Arlington, VA 22202.

FOR FURTHER INFORMATION CONTACT: Director, Identity Policy and Management, Office of Governmentwide Policy, Washington, DC 20405; or call 202-208-7655.

[[Page 56984]]

SUPPLEMENTARY INFORMATION: The General Services Administration's Federal Acquisition Service (FAS) is publishing a Privacy Act system of records notice to cover the collection, use, and maintenance of records relating to its administration of managed services in the collection and management of personally identifiable information for the purpose of issuing credentials (ID badges) to meet the requirements of Homeland Security Presidential Directive 12 for multiple agencies.

Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, required the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12

directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This policy is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 requires that the Federal credential be secure and reliable. As directed by the Presidential Directive, the National Institute of Standards and Technology (NIST) published the standard for secure and reliable forms of identification, Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, on February 25, 2005 and an update as FIPS 201-1 on June 26, 2006. HSPD-12 established four control objectives for Federal agencies to accomplish in implementing the directive:

Issue identification credentials based on sound criteria to verify an individual's identity;

Issue credentials that are strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation;

Provide for rapid, electronic authentication of personal identity; and

Issue credentials by providers whose reliability has been established through an official accreditation process.

FIPS 201 has two parts: PIV I and PIV II. The requirements in PIV I support the control objectives and identity verification and security requirements described in FIPS 201, including the requirement for standard background investigation for all Federal employees and long-term contractors. PIV II specifies standards for PIV credentials to support technical interoperability and security for all HSPD-12 deployments.

The Office of Management and Budget issued government-wide implementation guidance (M-05-24) for HSPD-12 on August 5, 2005. This implementation guidance required agencies to begin to issue identity credentials compliant with the PIV II requirements of FIPS 201 beginning October 27, 2006. OMB formed the HSPD-12 Executive Steering Committee (ESC) in November 2005 to establish broad direction to assist agencies in meeting HSPD-12 implementation requirements. As a key initiative to assist government-wide implementation efforts, the ESC asked for lead agencies to provide common infrastructure for agencies to share in meeting implementation requirements.

In response to the HSPD ESC direction, GSA established the HSPD-12 Managed Service Office (MSO) to provide common, shared infrastructure and services to assist Federal agencies in the implementation of HSPD-12. GSA is offering the HSPD-12 managed services on a government-wide basis; any agency can sign up to use the shared infrastructure and services. The scope of the GSA HSPD-12 managed services consist of enrollment services, systems infrastructure through a centralized PIV Identity Management System (IDMS), card production facility, and card activation, finalization and issuance. GSA will initially provide the HSPD-12 managed services in four locations to demonstrate the initial operating capability in Atlanta, New York City, Seattle, and Washington DC. All other localities within a Federal presence will be serviced over time. The managed services provide for the enrollment of applicants in the PIV program in compliance with FIPS PIV I requirements, the issuance of PIV II compliant PIV cards and credentials, and the maintenance of systems records. The initial operating capability will be a combination of manual and automated processes. Following the initial operating capability, GSA will begin to roll out enrollment stations and operating capability to additional

locations to service all user agencies.

The managed service PIV enrollment process and IDMS records will cover all user agency employees, contractors and their employees, consultants, and volunteers who require long-term, routine access to federal facilities, systems, and networks. The personal information to be collected in the enrollment process will consist of data elements necessary to verify the identity of the individual and to perform background or other investigations concerning the individual. The PIV IDMS will collect data elements from the PIV card applicant, including: Name, date of birth, Social Security Number, organizational and employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone number(s) as well additional verification and demographic information. These records also will be accessible to authorized personnel of participating Federal agencies for their PIV applicants. 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 personal information by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The GSA HSPD-12 Identity Management System is such a system of records. GSA will provide controlled access to the records of the PIV IDMS to participating Federal agencies for their PIV applicants. Participating agencies will need to determine whether any updates to their existing Privacy Act System of Records Notices are required.

Dated: September 21, 2006.
Cheryl Paige,
Acting Director, Office of Information Management.
GSA/GOVT-7

System Name:

Personal Identity Verification Identity Management System (PIV IDMS)

Security Classification:

Sensitive but unclassified.

System Location:

Records covered by this system are maintained by a contractor at the contractor's site.

Categories Of Individuals Covered By The System:

The PIV IDMS records will cover all participating agency employees, contractors and their employees, consultants, and volunteers who require routine, long-term access to federal facilities, information technology systems, and networks. The system also includes individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.).

At their discretion, participating Federal agencies may include short-term employees and contractors in the PIV

program and, therefore, inclusion in the PIV IDMS. Federal agencies shall make risk-based decisions to determine whether to issue PIV cards and require prerequisite background checks for short-term employees and contractors.

The system does not apply to occasional visitors or short-term guests. GSA and participating agencies will issue temporary identification and credentials for this purpose.

Categories Of Records In The System:

Enrollment records maintained in the PIV IDMS on individuals applying for the PIV program and a PIV credential through the GSA HSPD-12 managed service include the following data fields: full name; Social Security Number; Applicant ID number, date of birth; current address; digital color photograph; fingerprints; biometric template (two fingerprints); organization/office of assignment; employee affiliation; work e-mail address; work telephone number(s); office address; copies of identity source documents; employee status; military status; foreign national status; federal emergency response official status; law enforcement official status; results of background check; Government agency code; and PIV card issuance location. Records in the PIV IDMS needed for credential management for enrolled individuals in the PIV program include: PIV card serial number; digital certificate(s) serial number; PIV card issuance and expiration dates; PIV card PIN; Cardholder Unique Identifier (CHUID); and card management keys. Agencies may also choose to collect the following data at PIV enrollment which would also be maintained in the PIV IDMS: physical characteristics (e.g., height, weight, and eye and hair color).

Individuals enrolled in the PIV managed service will be issued a PIV card. The PIV card contains the following mandatory visual personally identifiable information: name, photograph, employee affiliation, organizational affiliation, PIV card expiration date, agency card serial number, and color-coding for employee affiliation. Agencies may choose to have the following optional personally identifiable information printed on the card: Cardholder physical characteristics (height, weight, and eye and hair color). The card also contains an integrated circuit chip which is encoded with the following mandatory data elements which comprise the standard data model for PIV logical credentials: PIV card PIN, cardholder unique identifier (CHUID), PIV authentication digital certificate, and two fingerprint biometric templates. The PIV data model may be optionally extended by agencies to include the following logical credentials: digital certificate for digital signature, digital certificate for key management, card authentication keys, and card management system keys. All PIV logical credentials can only be read by machine.

Authority For Maintenance Of The System:

5 U.S.C. 301; Federal Information Security Management Act (Pub. L. 107-296, Sec. 3544); E-Government Act (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al) and 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 Services Act of 1949, as amended.

Purposes:

The primary purposes of the system are: To ensure the safety and

security of Federal facilities, systems, or information, and of facility occupants and users; to provide for interoperability and trust in allowing physical access to individuals entering Federal facilities; and to allow logical access to Federal information systems, networks, and resources on a government-wide basis.

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 GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice (DOJ) when: (1) The agency or any component thereof; or (2) any employee of the agency in his or her official capacity; (3) 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 (4) 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 and 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: (1) The agency or any component thereof; (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where the agency or the Department of Justice has agreed to represent the employee; or (4) 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 and 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, SF 85-P, and SF 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 (NARA) 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, the Federal Information Security Management Act (Pub. L. 107-296), and

associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration.

g. To a Federal agency, State, local, foreign, or tribal or other public

[[Page 56986]]

authority, on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

h. To the Office of Management and Budget (OMB) 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; and applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

j. To designated agency personnel for controlled access to specific records for the purposes of performing authorized audit or authorized oversight and administrative functions. All access is controlled systematically through authentication using PIV credentials based on access and authorization rules for specific audit and administrative functions.

k. To the Office of Personnel Management (OPM) in accordance with the agency's responsibility for evaluation of Federal personnel management.

l. To the Federal Bureau of Investigation for the FBI National Criminal History check.

m. 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; and applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

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

Storage:

Records are stored in electronic media and in paper files.

Retrievability:

Records may be retrieved by name of the individual, Cardholder Unique Identification Number, Applicant ID, Social Security Number, and/or by any other unique individual identifier.

Safeguards:

Consistent with the requirements of the Federal Information

Security Management Act (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration, the GSA HSPD-12 managed service office protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a ``need to know'' basis, utilization of PIV Card access, secure VPN for web access, and locks on doors and approved storage containers. Buildings have security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include: Indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; biometric access screening. 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. All data is encrypted in transit. While it is not contemplated, any system records stored on mobile computers or mobile devices will be encrypted. GSA maintains an audit trail and performs random periodic reviews to identify unauthorized access. Persons given roles in the PIV process must be approved by the Government and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.

Retention And Disposal:

Disposition of records will be according to NARA disposition authority N1-269-06-1 (pending).

System Manager And Address:

Director, HSPD-12 Managed Service Office, Federal Acquisition Service (FAS), General Services Administration, Suite 911, 2011 Crystal Drive, Arlington, VA 22202.

Notification Procedure:

A request for access to records in this system may be made by writing to the System Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID.

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.

[FR Doc. E6-15901 Filed 9-27-06; 8:45 am]

BILLING CODE 6820-34-P