[Federal Register Volume 72, Number 47 (Monday, March 12, 2007)]
[Notices]
[Pages 11036-11040]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: E7-4407]

DEPARTMENT OF THE INTERIOR

Office of the Secretary

Privacy Act of 1974; as Amended; Amendments to an Existing System of Records

AGENCY: Office of the Secretary, Department of the Interior.

ACTION: Proposed amendment of an existing system of records.

SUMMARY: In accordance with the Privacy Act of 1974 (5 U.S.C. 552a), the Office of the Secretary of the Department of the Interior is issuing public notice of its intent to amend an existing Privacy Act system of records notice, Interior, OS-45, ``Security Clearance Files and Other Reference Files,'' to implement Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 requires Federal agencies to use a common identification credential for both logical and physical access to federally controlled facilities and information systems. Accordingly, the National Business Center, within the Office of the Secretary of the Department of the Interior, is implementing an identity management system to automate the process of issuing credentials to all Departmental employees, contractors, volunteers and other individuals who require regular, ongoing access to agency facilities and information systems and networks, based on sound criteria to verify an individual's identity, that are strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation, and that provide for rapid, electronic authentification of personal identity, by a provider whose reliability has been established through an official accreditation process. For this reason, it is renaming and renumbering Interior, OS-45, ``Security Clearance Files and Other Reference Files,'' as Interior, DOI-45: ``HSPD-12: Identity Management System and Personnel Security Files.''

DATES: Effective Date: U.S.C. 552a(e)(11) requires that the public be provided a 30-day period in which to comment on the agency's intended use of the information in the system of records. The Office of Management and Budget, in its Circular A-130, requires an additional 10-day period (for a total of 40 days) in which to make these comments. Any persons interested in commenting on this proposed amendment may do so by submitting comments in writing to the Office of the Secretary Privacy Act Officer, Sue Ellen Sloca, U.S. Department of the Interior, MS-120 SIB, 1951 Constitution Avenue, NW., Washington, DC 20240, or by e-mail to Sue_Ellen_Sloca@nbc.gov. Comments received within 40 days of publication in the Federal Register will be considered. The system will be effective as proposed at the end of the comment period unless comments are received which would require a contrary determination. The Department will publish a revised notice if changes are made based upon a review of comments received.

FOR FURTHER INFORMATION CONTACT: David VanderWeele, Security

Specialist, NBC Security Services, MS-1229 MIB, 1849 C St., NW., Washington, DC 20240, or by e-mail to David_A_Vanderweele@nbc.gov.

SUPPLEMENTARY INFORMATION: In this notice, the Department of the Interior is amending Interior, OS-45, ``Security Clearance Files and Other Reference Files'' to implement HSPD-12, and is renaming and renumbering it as Interior, DOI-45: ``HSPD-12: Identity Management System and Personnel Security Files.'' In the process, it is expanding the categories of individuals covered by the system to include all individuals who require regular, ongoing access to Departmental facilities and information systems and networks, and is expending the categories of records in the system to include additional personal identity verification (PIV) data such as fingerprints and copies of documents used to verify identification.

Note: This system notice also does not apply to individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department issues identification credentials, as a shared-service provider. Although data pertaining to these individuals are stored in the Department's identity management system, their records are covered, respectively, by their individual agency Privacy Act system of records notices.

Accordingly, the Department of the Interior proposes to amend the system notice for Interior, OS-45, ``Security Clearance Files and Other Reference Files'' in its entirety to read as follows:

Dated: March 7, 2007.
Sue Ellen Sloca,
Office of the Secretary Privacy Act Officer.
INTERIOR/DOI-45

System Name:
HSPD-12: Identity Management System and Personnel Security Files--Interior, DOI-45.

System Location:
Data covered by this system are maintained at the following locations:
(1) U.S. Department of the Interior, Office of the Secretary, National Business Center, 7301 West Mansfield Avenue, Mail Stop D-7200, Denver, CO 80225; U.S. Department of the Interior, Office of the Secretary, National Business Center, 1849 C St., NW., Mail Stop 1224 MIB, Washington, DC 20240.
(2) Bureau of Indian Affairs: Bureau of Indian Affairs, Office of Human Capital

[[Page 11037]]

Management, 1011 Indian School Road, NW., Mail Stop 64, Albuquerque, NM 87104.
(3) Bureau of Indian Education: Bureau of Indian Affairs, Office of Human Resources, P.O. Box 769, Albuquerque, NM 87103.
(4) Bureau of Land Management: Bureau of Land Management, Office of Law Enforcement and Security, 1620 L Street, NW., Washington, DC 20036.
(5) Bureau of Reclamation: Bureau of Reclamation, P.O. Box 25007, Denver, CO 80225.
(6) Minerals Management Service: Minerals Management Service, 381 Elden Street, Mail Stop 2050, Herndon, VA 20170.
(7) National Park Service: National Park Service, Office of Human Resources, 1201 Eye Street, NW., 12th Floor, Washington, DC 20005-5912.
(8) Office of Surface Mining, Reclamation and Enforcement: Office of Surface Mining, Reclamation and Enforcement, 1951 Constitution Avenue, NW., SIB, Washington, DC 20240.

(9) Office of the Inspector General: Office of the Inspector General, 12030 Sunrise Valley Drive, Suite 350, Mail Stop 5341, Reston, VA 20191.

(10) Office of the Secretary/National Business Center: See (1), above.

(11) Office of the Solicitor: Office of the Solicitor, Division of Administration, 1849 C St., NW., Mail Stop 6556 MIB, Washington, DC 20240.

(12) U.S. Fish and Wildlife Service: U.S. Fish and Wildlife Service, 4401 N. Fairfax Dr., Arlington, VA 22203.

(13) U.S. Geological Survey: U.S. Geological Survey, 250 National Center, 12201 Sunrise Valley Drive, Reston, VA 20192.

Categories Of Individuals Covered By The System:

(1) Individuals who require regular, ongoing access to Departmental facilities, information systems and networks, and/or information classified in the interest of national security, including applicants for employment or contracts with the Department of the Interior, Departmental employees, contractors, students, interns, volunteers, affiliates, and individuals formerly in any of these positions. The system also covers individuals authorized to perform or use services provided in Departmental facilities (e.g., Credit Union, Fitness Center, etc.)

Note: This system notice does not apply to occasional visitors or short-term guests to whom the Department issues temporary identification and credentials. These records are covered by Interior/DOI-46, ``HSPD-12: Physical Security System Files.'' This system notice also does not apply to individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department issues identification credentials, as a shared-service provider. Although data pertaining to these individuals are stored in the Department's identity management system, their records are covered, respectively, by their individual agency Privacy Act system of records notices. Additionally, this system notice does not apply to individuals accused of security violations or found to be in violation. Records relating to personnel and building security violations will be covered by Interior/OS-18: ``Security Complaints and Investigations Files.''

(2) Employees of independent agencies, councils and commissions (which are provided administrative support by the Department of the Interior), whose duties have been designated ``special sensitive,'' ``critical sensitive,'' ``noncritical sensitive'' or ``clearance for FEMA special access program.''

(3) Individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department provides enrollment services but not identification credentials.

Note: Information on these individuals is maintained for the minimum time required to process it before secure transmission to another agency's identity management system through a third party enrollment broker. Records pertaining to these individuals are covered, respectively, by their individual agency Privacy Act system of records notices.

Categories Of Records In The System:

(1) Copies of forms SF 85, SF 85P, SF 85P-S, SF 86, SF 86A, SF 86C, and FD 258 as supplied by individuals covered by the system.

(2) Name, former names, birth date, birth place, Social Security Number, signature, home address, e-mail address, phone numbers, employment history, residential history, education and degrees earned, names of associates and references and their contact information,

citizenship, names of relatives, birthdates and places of relatives, citizenship of relatives, names of relatives who work for the Federal government, criminal history, mental health history, drug use, financial information, fingerprints, summary report of investigation, results of suitability decisions, level of security clearance, date of issuance of security clearance, and requests for appeal.

(3) Copies of letters of transmittal between the Department of the Interior and the Office of Personnel Management concerning the covered individual's background investigation, and copies of certification of clearance status and briefings and/or copies of debriefing certificates signed by the individual, as appropriate. Card files contain case file summaries, case numbers and dispositions of case files following review.

(4) Copies of personal identity verification (PIV) application forms as supplied by individuals covered by the system.

(5) Records maintained on individuals issued credentials by the Department include the following data fields: Full name, Social Security Number; date of birth; signature; image (photograph); fingerprints; hair color; eye color; height; weight; home address; work address; e-mail address; agency affiliation (i.e., employee, contractor, volunteer, etc.); telephone numbers; PIV card issue and expiration dates; personal identification number (PIN); results of background investigation; PIV request form; PIV registrar approval signature; PIV card serial number; emergency responder designation; copies of ``I-9'' documents (e.g., driver's license, passport, birth certificate, etc.) used to verify identification or information derived from those documents such as document title, document issuing authority, document number, or document expiration date; level of national security clearance and expiration date; computer system user name; user access and permission rights, authentication certificates; and digital signature information.

Authority For Maintenance Of The System:

Executive orders 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42; U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; 5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, section 203); the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and the Federal Property and Administrative Act of 1949, as amended.

[[Page 11038]]

Routine Uses Of Records Maintained In The System, Including Categories Of Users And The Purposes Of Such Uses.

The primary purposes of the system are:

(1) To document and support decisions regarding

(a) Clearance for access to classified information;

(b) Suitability, eligibility, and fitness for service of applicants for Federal employment and contract positions, including students, interns, or volunteers to the extent their duties require regular, ongoing access to Departmental facilities and information systems and networks; and

(2) To verify the identity of individuals issued common identification credentials by the Department in compliance with the HSPD-12 directive.

(3) To ensure the safety and security of Departmental facilities and information systems and networks, and their occupants and users.

Note: This system interfaces with the Department's physical security system, covered by Interior/DOI-46, ``HSPD-12: Physical

Security Files,'' and the Department's logical security system, covered by Interior/DOI-47, ``HSPD-12: Logical Security Files (Enterprise Access Control Service / EACS).'' This system will also interface with the Department's Federal Payroll and Personnel System (FPPS), covered by Interior/DOI-85, ``Payroll, Attendance, Retirement, and Leave Records.''

Disclosures outside the Department of the Interior may be made:

(1) To the Office of Personnel Management for matters concerned with oversight activities (necessary for the Office of Personnel Management to carry out its legally-authorized Government-wide personnel management programs and functions.)

(2)(a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:

(i) The U.S. Department of Justice (DOJ);

(ii) A court or an adjudicative or other administrative body;

(iii) A party in litigation before a court or an adjudicative or other administrative body; or

(iv) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;

(b) When:

(i) One of the following is a party to the proceeding or has an interest in the proceeding:

(A) DOI or any component of DOI;

(B) Any other Federal agency appearing before the Office of Hearings and Appeals;

(C) Any DOI employee acting in his or her official capacity;

(D) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;

(E) The United States, when DOJ determines that DOI is likely to be affected by the proceeding; and

(ii) DOI deems the disclosure to be:

(A) Relevant and necessary to the proceeding; and

(B) Compatible with the purpose for which the records were compiled.

(3) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the congressional office about the individual.

(4) To the Federal Protective Service and appropriate Federal, State, local or foreign agencies responsible for investigating emergency response situations or investigating or prosecuting the violation of or for enforcing or implementing a statute, rule, regulation, order or license, when DOI becomes aware of a violation or potential violation of a statute, rule, regulation, order or license.

(5) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected and maintained.

(6) To Federal, State, or local agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee, contractor, etc., or the issuance of a security clearance, license, contract, grant or other benefit.

(7) To representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2903 and 2904.

(8) To state and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation.

(9) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs, on DOI's behalf, services requiring access to these records.

(10) To the Office of Management and Budget when necessary to the

review of private relief legislation pursuant to OMB Circular No. A-19.

(11) To other Federal agencies through third party enrollment brokers serving as links in the secure chain of custody for the HSPD-12 process when the Department has entered into agreements with these agencies to provide enrollment services to their employees, contractors, etc. but not identification credentials.

Note: In all such instances, the data being disclosed to these agencies through the enrollment brokers is data pertaining to their own employees, contractors, etc., and not data pertaining to Departmental employees, contractors, etc.

(12) To the Federal Bureau of Investigation for the National Agency Check with Inquiries (NACI) background investigation.

(13) To appropriate agencies, entities, and persons when:

(a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; and

(b) The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(c) The disclosure is made to such agencies, entities and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Pursuant to 5 U.S.C. 552a(b)(12), records can be disclosed to consumer reporting agencies as they are defined in the Fair Credit Reporting Act.

Policies And Practices For Storing, Retrieving, Accessing, Retaining, And Disposing Of Records In The System:

Storage:

Records are stored in paper files and in electronic media.

Retrievability:

Records are retrievable by name of employee or covered individual, Social Security Number, other ID number, PIV card serial number, image (photograph), or fingerprint.

Safeguards:

Access to records covered by the system will be permitted only to authorized personnel in accordance with requirements found in the Departmental Privacy Act regulations (43 CFR 2.51). Persons given roles in the PIV process must complete training

[[Page 11039]]

specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information regardless of how and where it is stored. Paper records are stored in locked file cabinets in a secure area. Electronic records in the identity management system are maintained with safeguards meeting the requirements of 43 CFR 2.51 for automated records, which conform to Office of Management and Budget and Departmental guidelines reflecting the implementation of the Federal Information Security Management Act. The electronic data are protected through user identification, passwords, database permissions, encryption and software controls. Such security measures establish different degrees of access levels for different types of users. An

audit trail is maintained and reviewed periodically to identify unauthorized access. A Privacy Impact Assessment was completed to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met.

Retention And Disposal:

Although paper records relating to individuals covered by the system are generally retained and disposed of in accordance with General Records Schedule 18, Item 22, approved by the National Archives and Records Administration, a separate records schedule, identified as item 6600 of the Office of the Secretary Consolidated Subject-Function Code Records Disposition Schedule is under development. This schedule prescribes that records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

Additionally, in accordance with HSPD-12, PIV Cards are deactivated within 18 hours of notification regarding cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

System Manager(S) And Address:

(1) HSPD-12 System Manager:

Security Manager, U.S. Department of the Interior, Office of the Secretary, National Business Center, 1849 C St., NW., Mail Stop 1229 MIB, Washington, DC 20240.

(2) Bureau Personnel Security System Managers:

(a) Bureau of Indian Affairs:

Security Program Supervisor, Bureau of Indian Affairs, Office of Human Capital Management, 1011 Indian School Road, NW., Mail Stop 64, Albuquerque, NM 87104.

(b) Bureau of Indian Education:

Personnel Security Specialist, Bureau of Indian Education, Office of Human Resources, P.O. Box 769, Albuquerque, NM 87103.

(c) Bureau of Land Management:

Chief Security and Intelligence, Bureau of Land Management, Office of Law Enforcement and Security, 1620 L Street, NW., Washington, DC 20036.

(d) Bureau of Reclamation:

Security Specialist, Bureau of Reclamation, P.O. Box 25007, Denver, CO 80225.

(e) Minerals Management Service:

Personnel Security Specialist, Minerals Management Service, 381 Elden Street, Mail Stop 2050, Herndon, VA 20170.

(f) National Park Service:

Security Officer, National Park Service, Office of Human Resources, 1201 Eye Street, NW., 12th Floor, Washington, DC 20005-5912.

(g) Office of Surface Mining, Reclamation and Enforcement:

Personnel Security Officer, Office of Surface Mining, Reclamation and Enforcement, 1951 Constitution Avenue, NW., SIB, Washington, DC 20240.

(h) Office of the Inspector General:

Security Specialist, Office of the Inspector General, 12030 Sunrise Valley Drive, Suite 350, Mail Stop 5341, Reston, VA 20191.

(i) Office of the Secretary/National Business Center:

Security Manager, National Business Center, MS-1224 MIB, 1849 C St., NW., Washington, DC 20240.

(j) Office of the Solicitor:

Director of Administrative Services, Division of Administration, Office of the Solicitor, 1849 C St., NW., MS-6556, Washington, DC 20240.

(k) U.S. Fish and Wildlife Service:

Personnel Security Manager, U.S. Fish and Wildlife Service, 4501 N. Fairfax Dr., 3rd Fl., Arlington, VA 22203.

(1) U.S. Geological Survey:
Bureau Security Manager, U.S. Geological Survey, 250 National Center, 12201 Sunrise Valley Drive, Reston, VA 20192.

Notification Procedure:
A request for notification of the existence of electronic records pertaining to the HSPD-12 credentialing process shall be addressed to the HSPD-12 System Manager identified in (1) above. A request for notification of the existence of paper records pertaining to the personnel security management process shall be addressed to the appropriate Bureau Personnel Security System Manager identified in (2), above. All such requests for notification must be in writing, signed by the requester, include the requester's bureau and office affiliation and work address, if an employee, or the name and address of the bureau and office with whom the requester is associated for purposes of identity credentialing, and address of the facility or name of the system that the requester needed access to, to facilitate location of applicable paper records, if inquiring about paper records, and comply with the content requirements of 43 CFR 2.60.

Note: Individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department issues identification credentials, as a shared-service provider, requesting notification of the existence of identity management and personnel security records pertaining to themselves, must contact the appropriate party identified in this section of the Privacy Act system of records notice published by the agency with which they are affiliated.

Record Access Procedure:
A request for access to or copies of electronic records pertaining to the HSPD-12 credentialing process shall be addressed to the HSPD-12 System Manager identified in (1) above. A request for access to or copies of paper records pertaining to the personnel security management process shall be addressed to the appropriate Bureau Personnel Security System Manager identified in (2), above. All such requests must be in writing, signed by the requester, include the requester's bureau and office affiliation and work address, if an employee, or the name and address of the bureau and office with whom the requester is associated for purposes of identity credentialing, and address of the facility or name of the system that the requester needed access to, to facilitate location of applicable paper records, if inquiring about paper records, and comply with the content requirements of 43 CFR 2.63.

Note: Individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department issues identification credentials, as a shared-service provider, requesting access to or copies of identity management and personnel security records pertaining to themselves, must contact the appropriate party identified in this section of the Privacy Act system of records notice published by the agency with which they are affiliated.

[[Page 11040]]

Contesting Records Procedure:
A request for amendment of electronic records pertaining to the HSPD-12 credentialing process shall be addressed to the HSPD-12 System Manager identified in (1) above. A request for amendment of paper records pertaining to the personnel security management process shall be addressed to the appropriate Bureau Personnel Security System

Manager identified in (2), above. All such requests must be in writing, signed by the requester, include the requester's bureau and office affiliation and work address, if an employee, or the name and address of the bureau and office with whom the requester is associated for purposes of identity credentialing, and address of the facility or name of the system that the requester needed access to, to facilitate location of applicable paper records, if inquiring about paper records, and comply with the content requirements of 43 CFR 2.71.

Note: Individuals who require regular, ongoing access to facilities and information systems and networks managed by other Federal agencies on whose behalf the Department issues identification credentials, as a shared-service provider, requesting amendment of identity management and personnel security records pertaining to themselves, must contact the appropriate party identified in this section of the Privacy Act system of records notice published by the agency with which they are affiliated.

Record Source Categories:

Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the SF-85, SF-85P, SF-86, SF-87A and FD 258 and personal interviews; employers' and former employers' records; other Federal agencies supplying data on covered individuals; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions. Other Federal agencies providing HSPD-12 enrollment services to Department of the Interior employees, contractors, etc. through third party enrollment brokers.

Exemptions Claimed For The System:

None.

[FR Doc. E7-4407 Filed 3-9-07; 8:45 am]
BILLING CODE 4310-RK-P