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

DEPARTMENT OF THE INTERIOR

Office of the Secretary

Privacy Act of 1974, as Amended; Amendment of 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 is issuing public notice of its intent to amend an existing Privacy Act system of records notice, Interior, DOI—30, ''Enterprise Access Control Service (EACS),'' 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 planning to link, via Web services, its enterprise information technology directory, the Enterprise Access Control Service (EACS), with the identity management system (operated by the National Business Center) which automates the process of issuing HSPD–12 compliant credentials to all Departmental employees, contractors, volunteers and other individuals who require regular, ongoing access to agency facilities, 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, DOI–30, ''Enterprise Access Control Service (EACS)'' as Interior, DOI–47: ''HSPD–12: Logical Security Files (Enterprise Access Control Service/EACS).''

DATES: *Effective Date:* 5 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: Richard A. Delph, Office of the Chief Information Officer, Office of the Secretary, Department of the Interior, 625 Herndon Parkway, Herndon, VA 20170 or by e-mail to *Richard_Delph@ios.doi.gov*.

SUPPLEMENTARY INFORMATION: In this notice, the Department of the Interior is amending Interior, DOI–30, ''Enterprise Access Control Service (EACS),'' to implement HSPD–12, and is renaming and renumbering it as Interior, DOI–47: ''HSPD–12: Logical Security Files (Enterprise Access Control Service/EACS).'' In the process, it is expanding the categories of individuals covered by the system to include all individuals authorized to access DOI systems and networks, e.g., volunteers and other individuals who require regular, ongoing access to Departmental information systems and networks, individuals who have been issued HSPD–12 compliant credentials from other Federal agencies who require access to Departmental information systems and networks, etc.

Accordingly, the Department of the Interior proposes to amend the system notice for Interior, DOI–30, ''Enterprise Access Control Service (EACS)'' in its entirety to read as follows:

Dated: March 7, 2007.

Sue Ellen Sloca,

Office of the Secretary Privacy Act Officer.

INTERIOR/DOI–47

SYSTEM NAME:

HSPD–12: Logical Security Files (Enterprise Access Control Service/EACS)—Interior, DOI–47

SYSTEM LOCATION:

(1) Data covered by this system are maintained at two primary master sites at the following locations under the Department of the Interior (DOI), Office of the Secretary, Office of the Chief Information Officer, at:

(a) The Enterprise Hosting Center, Reston, VA, and

(b) The Enterprise Hosting Center, Denver, CO.

(2) DOI bureau and office replicas of the master database of the EACS are located at strategic Departmental locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individuals who require access to Departmental networks, information systems, and e-mail services, including Departmental employees, contractors, students, interns, volunteers, etc.

Note: All of these individuals are required to have HSPD–12 compliant credentials issued from the National Business Center, within the Office of the Secretary of the Department of the Interior, if they are employed by DOI for more than 180 days.

(2) Individuals who have been issued HSPD–12 compliant credentials from other Federal agencies who require access to Departmental networks, information systems and e-mail services.

CATEGORIES OF RECORDS IN THE SYSTEM:

The following information may be retained in EACS: User full legal name, system login name, work e-mail address, web home page address, work address, work phone number, other contact information, user access and permission rights, password hash values, HSPD–12 authentication, digital signature, encryption, and/or other NIST specified certificates, along with the date and time of signature retained on the signed document, and supervisor's name.

Note: This list is not intended to be a full list of all information currently stored in the EACS.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 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 Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

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 provide a common authoritative directory service for the purpose of ensuring the security of DOI computer networks, resources and information and protecting them from unauthorized access, tampering or destruction;

(2) To authenticate and verify that all persons accessing DOI computer networks, resources and information are properly authorized to access them;

(3) To ensure that persons signing official digital documents are indeed the persons represented and to provide for non-repudiation of the use of an electronic signature; and

(4) To enable an individual to encrypt and decrypt documents for secure transmission.

Note: This system interfaces with the Department's identify management system and personnel security files, covered by Interior/DOI–45, ''HSPD–12: Identity Management System and Personnel Security Files.''

DISCLOSURES OUTSIDE THE DEPARTMENT OF THE INTERIOR MAY BE MADE:

(1) 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.

(2) 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.

(3) (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.

(4) 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.

(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 representatives of the General Services Administration or the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2903 and 2904.

(7) 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.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are stored in electronic media on hard disks and magnetic tapes.

RETRIEVABILITY:

Records are retrievable from EACS by any defined field within the record. These fields include, but are not limited to: user name, full legal name, digital certificate, and Web home address or e-mail address.

SAFEGUARDS:

The computer systems in which records are stored are located in computer facilities that are secured by alarm systems and off-master key access. EACS access granted to

individuals is password-protected. In the event that EACS is used to validate a user's authentication certificate against existing data within the system, access to the user's authentication certificate will require the use of a Personal Identification Number (PIN) known only to the user. Each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice will appear on the monitor screen when first displayed. Backup tapes are transported in a locked container under armed guard escort and are stored in a locked and controlled room in a secure, off-site location. A Privacy Impact Assessment was completed to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met.

RETENTION AND DISPOSAL:

Records relating to persons covered by this system are retained in accordance with a separate records schedule, identified as item 6600 of the Office of the Secretary Consolidated Subject-Function Code Records Disposition Schedule currently under development.

SYSTEM MANAGER(S) AND ADDRESS:

(1) EACS Manager, Office of the Chief Information Officer, Office of the Secretary, Department of the Interior, 625 Herndon Parkway, Herndon, VA 20170.

(2) Bureau Security Managers:

a. Bureau of Indian Affairs: Director, Office of Information Technology Security & Privacy, Office of the Chief Information Officer—Indian Affairs, 625 Herndon Parkway, Herndon, VA 20170.

b. Bureau of Indian Education: Director, Office of Information Technology Security & Privacy, Office of the Chief Information Officer—Indian Affairs, 625 Herndon Parkway, Herndon, VA 20170.

c. Bureau of Land Management: Division Chief, IT Security, Bureau of Land Management, Information Resources Management, 1849 C St., NW., Mail Stop 700LS, Washington, DC 20240.

d. Bureau of Reclamation: Deputy Chief Information Officer, Bureau of Reclamation, P.O. Box 25007, Denver, CO 80225.

e. Minerals Management Service: IT Specialist, Minerals Management Service, 381 Elden Street, Mail Stop 2200, Herndon, VA 20170.

f. National Park Service: Security Program Manager, National Park Service, 1201 Eye Street, NW., Washington, DC 20005.

g. Office of Surface Mining, Reclamation and Enforcement: Logical Security Officer, Office of Surface Mining, Reclamation and Enforcement, 1951 Constitution Ave., NW., Mail Stop 344 SIB, Washington, DC 20240.

h. Office of the Inspector General: Logical Security Manager, U.S. Geological Survey, 12030 Sunrise Valley Drive, Suite 230, Reston, VA 20191.

i. Office of the Secretary/National Business Center: Logical Security Manager, National Business Center, 7301 W. Mansfield Ave., D 2130, Denver, CO 80235.

j. Office of the Solicitor: Chief Information Officer, Division of Administration, Office of the Solicitor, 1849 C St., NW., Mail Stop 6556 MIB, Washington, DC 20240.

k. U.S. Fish and Wildlife Service: AD IRTM, U.S. Fish and Wildlife Service, 4401 N. Fairfax Dr., 3rd Fl., Arlington, VA 22203.

l. U.S. Geological Survey: Bureau Chief Technology Officer, U.S. Geological Survey, 8987 Yellow Brick Road, Baltimore, MD 21237.

NOTIFICATION PROCEDURE:

An individual requesting notification of the existence of records on himself or herself should address his/her request to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing and signed by the requester. It must include the requester's full name, bureau and office affiliation, and work address. (See 43 CFR 2.60.)

RECORD ACCESS PROCEDURE:

An individual requesting access to records on himself or herself should address his/her request to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing and signed by the requester. It must include the requester's full name, bureau and office affiliation, and work address. (See 43 CFR 2.63.)

CONTESTING RECORDS PROCEDURE:

An individual requesting amendment of records on himself or herself should address his/her request to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing and signed by the requester. It must include the requester's full name, bureau and office affiliation, and work address. (See 43 CFR 2.71.)

RECORD SOURCE CATEGORIES:

Information is obtained from individuals covered by the system, supervisors, and designated approving officials, certificate issuing authorities, and network systems officials, as well as the National Business Center's identity management system (covered by Interior, DOI–45: ''HSPD–12: Identity Management System and Personnel Security Files).''

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E7–4408 Filed 3–9–07; 8:45 am]

BILLING CODE 4310–RK–P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

Privacy Act of 1974; as Amended; Deletion of an Existing System of Records

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

ACTION: Proposed deletion 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 delete an existing Privacy Act system of records notice, Interior, DOI–15, ''Authenticated Computer Access and Signature System.'' It was previously published in the **Federal Register** on January 5, 2005 (70 FR 1262). Records covered by this notice are being incorporated into an amendment of Interior, OS–45, ''Security Clearance Files and Other Reference Files,'' which is being updated to implement Homeland Security Presidential Directive 12 (HSPD–12), and is being renamed and renumbered as Interior, DOI–45, ''HSPD–12: Identity Management System and Personnel Security Files.'' HSPD–12 requires Federal agencies to use a common identification credential for both logical and physical access to federally controlled facilities and information systems.

DATES: *Effective Date:* 5 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. Because records covered by this notice are still being collected and maintained by the Department of the Interior, this deletion notice will be effective at the end of the comment period for Interior, DOI–45, HSPD–12: ''Identity Management System and Personnel Security Files,'' which is being published concurrently with this deletion notice, unless comments are