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

received which would require a contrary determination vis-à-vis Interior, DOI–45. Should the Department receive comments that require that it republish Interior, DOI–45, this deletion notice will be effective on the date on which the revised notice for Interior, DOI–45 becomes effective.

FOR FURTHER INFORMATION CONTACT: Sue Ellen Sloca, Office of the Secretary Privacy Act Officer, 1951 Constitution Avenue, NW., MS–120 SIB, Washington, DC 20240, at 202–208–6045, or by e-mail to *sue_ellen_sloca@nbc.gov.*

Signed: March 7, 2007.

Sue Ellen Sloca,

Office of the Secretary Privacy Act Officer.

[FR Doc. E7–4413 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, OS–01, ''Computerized ID Security System,'' to implement Homeland Security Presidential Directive 12 (HSPD–12) and to clarify its interpretation of 5 U.S.C. 6106. 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 integrating its computerized smart-card physical security system with the identity management system which automates the process of issuing 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. It is also expanding the coverage of this system to include all locations, Departmentwide, both Federal buildings and Federally-leased space, where paper-based physical security logs and registers have been established, in addition to or in place of smart-card access control systems. For this reason, it is renaming and renumbering this Privacy Act system notice as Interior, DOI–46: ''HSPD–12: Physical Security Files.''

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: 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 (DOI) is amending Interior, OS–01, ''Computerized ID Security System'' to implement HSPD–12, and is renaming and renumbering it as Interior, DOI–46: ''HSPD–12: Physical Security Files.'' In the process, it is expanding the categories of individuals covered by the system to include all individuals who have access to DOI facilities, and the categories of records covered by the system notice to include additional personal identity verification (PIV) data such as fingerprints. It is also clarifying its interpretation of 5 U.S.C. 6106 by deleting the note that follows the list of the routine uses of the records maintained in the system. This note concerned disclosures within DOI of data pertaining to the date and time of entry and exit of an agency employee working in the District of Columbia.

Accordingly, the Department of the Interior proposes to amend the system notice for Interior, OS–01, ''Computerized ID Security System'' in its entirety to read as follows:

Dated: March 7, 2007.

Sue Ellen Sloca,

Office of the Secretary Privacy Act Officer.

INTERIOR/DOI–46

SYSTEM NAME:

HSPD–12: Physical Security Files—Interior, DOI–46.

SYSTEM LOCATION:

(1) Data covered by this system are maintained at the following main locations:

(a) U.S. Department of the Interior, Office of the Secretary, National Business Center, Computer Center, 1849 C Street, NW., Washington, DC 20240; and

(b) U.S. Department of the Interior, Office of the Secretary, National Business Center, 7301 W. Mansfield Ave., MS D–2130, Denver, CO 80235–2300.

(2) Portions of the data covered by this system are also maintained at other Department of the Interior locations, both Federal buildings and Federally-leased space, where staffed guard stations have been established in facilities that have installed a smart card ID system, and/or paper-based physical security logs and registers, as well as the physical security office(s) of those locations. A list of these locations (as applicable to each bureau) is maintained by each bureau's Security Manager, whose address is provided under item (2) in System Manager and Address, below.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individuals who require regular, ongoing access to Departmental facilities, including Departmental employees, contractors, students, interns, volunteers, affiliates, and individuals formerly in any of these positions. The system also includes individuals authorized to perform or use services provided in Departmental facilities (e.g., Credit Union, Fitness Center, 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