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

other Federal agencies who require access to Departmental facilities.

(3) Visitors and other individuals who require infrequent access to Department facilities including services provided in Departmental facilities (e.g., Departmental Museum, Indian Arts and Crafts Shop, etc.)

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Records maintained on individuals issued HSPD–12 compliant credentials by the Department and by other Federal agencies 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 number; personal identity verification (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.

(2) Records maintained on visitors and other individuals who require infrequent access to Department facilities include the following data fields: Full name, signature; image (photograph), Social Security Number (or one of the following: Driver's License number, ''Green Card'' number, Visa number, or other ID number), images of relevant ID document(s), U.S. Citizenship (yes or no/logical data field), date of entry, time of entry, location of entry, time of exit, location of exit, purpose for entry, agency point of contact, company name, security access category, and access status.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 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); Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; 5 U.S.C. 301; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

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 ensure the safety and security of DOI facilities and their occupants in which the system is installed.

(2) To verify that all persons entering DOI facilities or other Government facilities with smart card systems are authorized to enter them.

(3) To verify that all persons entering DOI facilities or other Government facilities without smart cards are authorized to enter them.

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) To another agency with a similar HSPD–12 (PIV/smart card) system when a person with identification credentials issued by the Department desires access to that agency's facilities.

(4) (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.

(5) 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.

(6) 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.

(7) 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.

(8) To another agency with a similar HSPD–12 (PIV/smart card) system when it controls access to facilities occupied by the agency.

(9) 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 and in paper files.

RETRIEVABILITY:

Records are retrievable by name, Social Security Number, other ID number, image (photograph), fingerprint, organization/office of assignment, agency point of contact, company name, security access, category, date of entry, time of entry, location of entry, time of exit, location of exit, ID security card issue date, ID security card expiration date, and ID security card serial number.

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). Paper records are stored in locked file cabinets in a secure area. Electronic records 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 computer servers in which records are stored are located in computer facilities that are secured by alarm systems and off-master key access. The computer servers themselves are password-protected. Access granted to individuals at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the client PCs at the guard stations and badging office are encrypted. Backup tapes 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 General Records Schedule 18, Item No. 17. Unless retained for specific, ongoing security investigations:

(1) Records relating to individuals other than employees are destroyed two years after ID security card expiration date.

(2) Records relating to date and time of entry and exit of employees are destroyed two years after date of entry and exit.

(3) All other records relating to employees are destroyed two years after ID security card expiration date.

SYSTEM MANAGER(S) AND ADDRESS:

(1) Security Manager, Physical Security Office, Division of Employee and Public Services, National Business Center, MS–1224, 1849 C Street, NW, Washington, DC 20240.

(2) Bureau Physical Security Managers:

(a) Bureau of Indian Affairs: Indian Affairs Homeland Security Coordinator, 1849 C St., NW., Mail Stop 4160 MIB, Washington, DC 20240.

(b) Bureau of Indian Education: Indian Affairs Homeland Security Coordinator, 1849 C St., NW., Mail Stop 4160 MIB, Washington, DC 20240.

(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: Reclamation Security 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 2050, Herndon, VA 20170.

(f) National Park Service: Law Enforcement, Security and Emergency Service Manager, National Park Service, Security and Intelligence Branch, 1201 I (Eye) St., NW., 10th Floor, Washington, DC 20005.

(g) Office of Surface Mining, Reclamation and Enforcement: 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: Support Services Supervisor, 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: Office of the Secretary/ National Business Center: Security Manager, National Business Center, Mail Stop 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., Mail Stop 6556 MIB, Washington, DC 20240.

(k) U.S. Fish and Wildlife Service: Security and Emergency Manager, U.S. Fish and Wildlife Service, 4401 N. Fairfax Dr., Arlington, VA 22203.

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

NOTIFICATION PROCEDURE:

An individual requesting notification of the existence of records on himself or herself maintained at either of the two main system locations should address his/her request to the Security Manager identified in (1), above. A request for notification of the existence of physical security records located at any other location should be addressed to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing, signed by the requester, and include the requester's bureau and office affiliation and the address of the facility to which the requester needed access to facilitate location of the applicable records. (See 43 CFR 2.60.)

RECORD ACCESS PROCEDURE:

An individual requesting access to records maintained on himself or maintained at either of the two main system locations should address his/her request to the Security Manager identified in (1), above. A request for access to physical security records located at any other location should be addressed to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing, signed by the requester, and include the requester's bureau and office affiliation and the address of the facility to which the requester needed access to facilitate location of the applicable records. (See 43 CFR 2.63.)

CONTESTING RECORDS PROCEDURE:

An individual requesting amendment of a record maintained on himself or herself at either of the two main system locations should address his/her request to the Security Manager identified in (1), above. A request for amendment of physical security records located at any other location should be addressed to the appropriate Bureau Security Manager identified in (2), above. The request must be in writing, signed by the requester, and include the requester's bureau and office affiliation and the address of the facility to which the requester needed access to facilitate location of the applicable records. (See 43 CFR 2.71.)

RECORD SOURCE CATEGORIES:

Information is obtained from individuals covered by the system,

supervisors, and designated approving officials, as well as records supplied by the National Business Center's identity management system, other Federal agencies issuing HSPD–12 compliant cards, and HSPD–12 compliant cards carried by individuals seeking access to Departmental and other Federal facilities occupied by agency employees.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E7–4414 Filed 3–9–07; 8:45 am]

BILLING CODE 4310–RK–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

Post-delisting Monitoring Plan for Eggert's Sunflower (Helianthus eggertii)

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of document availability.

SUMMARY: We, the Fish and Wildlife Service, announce the availability of the Post-delisting Monitoring Plan for Eggert's sunflower (*Helianthus eggertii*) (Monitoring Plan). The status of Eggert's sunflower will be monitored over a 5-year period from 2006 through 2010, through annual evaluation of information routinely being collected by seven agencies that have entered into long-term management agreements with us covering 27 populations of Eggert's sunflowers, combined with a total census of these populations during the second and fifth year of the monitoring period.

ADDRESSES: Copies of the Monitoring Plan are available by request from the Field Supervisor, Fish and Wildlife Service, 446 Neal Street, Cookeville, Tennessee 38501 (telephone 931–528–6481; fax: 931–528–7074). This Monitoring Plan is also available on the World Wide Web at *http://www.fws.gov/cookeville*.

FOR FURTHER INFORMATION CONTACT: Geoff Call, Recovery Coordinator, at the above Cookeville address, at *geoff_call@fws.gov*, or at 931/528–6481, extension 213.

SUPPLEMENTARY INFORMATION:

Background

Eggert's sunflower is a perennial member of the aster family (Asteraceae) known only from Alabama, Kentucky, and Tennessee. The species is commonly associated with the barrens/woodland ecosystem. It occurs on rolling-to-flat uplands and in full sun or partial shade. It is often found in open fields or in thickets along woodland borders and with other tall herbs and small trees. It persists in, and may even invade, roadsides, power line rights-of-way, or fields that have suitable open habitat.

Eggert's sunflower was listed as threatened under the Endangered Species Act (Act) on May 22, 1997 (62 FR 27973). At the time of listing, there were 34 known Eggert's sunflower sites occurring in 1 site in 1 county in Alabama, 13 sites in 5 counties in Kentucky, and 20 sites in 8 counties in Tennessee. When the Recovery Plan for this species was finalized in 1999, there was 1 known site in Alabama, 27 sites in 6 counties in Kentucky, and 203 sites in 12 counties in Tennessee. Presently, there are 287 known Eggert's sunflower sites distributed across 3 counties in Alabama, 9 counties in Kentucky, and 15 counties in Tennessee.

On August 18, 2005, we published a final rule removing Eggert's sunflower from the Federal List of Endangered and Threatened Wildlife and Plants (70 FR 48482). Our decision to delist this species was based on a review of all available data, which indicated that the species was more widespread and abundant than was documented at the time of listing, was more resilient and less vulnerable to certain activities than previously thought, and is now protected on Federal, State, and county lands.

Section 4(g)(1) of the Act requires that we implement a system, in cooperation with the States, to monitor all species that have been delisted, or removed from the Federal List of Endangered and Threatened Wildlife and Plants, due to recovery for at least 5 years following delisting. The purpose of this post-delisting monitoring is to verify that a species delisted due to recovery remains secure from risk of extinction after it no longer has the protections of the Act. In keeping with that mandate, we developed this Monitoring Plan in cooperation with the States of Alabama, Kentucky, and Tennessee. We are responsible for compliance with section 4(g) and must remain actively engaged in all phases of the post-delisting monitoring.

The Draft Post-delisting Monitoring Plan for Eggert's sunflower was available for public comment from August 18, 2005 through September 19, 2005 (70 FR 48577). The only response we received was from the State of Tennessee, which supported the plan. Since we had no additional information provided to us during the comment period, we have finalized the Post-delisting Monitoring Plan with no changes from the draft.

The Monitoring Plan is designed to track the population status of Eggert's sunflower by using information routinely collected by our partners on a yearly basis as well as a total population census during the second and fifth years of the monitoring period for the 27 populations that occur on public lands. We will also annually evaluate the effectiveness of the Cooperative Management Agreements in protecting Eggert's sunflower populations on these public lands.

If we determine at the end of the 5-year post-delisting monitoring period that ''recovered'' status is still appropriate and factors that led to the listing of Eggert's sunflower, or any new factors, remain sufficiently reduced or eliminated, monitoring may be reduced or terminated. If data show that the species is declining or if one or more factors that have the potential to cause a decline are identified, we will continue monitoring beyond the 5-year period and may modify the Monitoring Plan based on an evaluation of the results of the initial Monitoring Plan, or reinitiate listing if necessary.

Author

The primary author of this proposed rule is Geoff Call (see **ADDRESSES** section).

Authority

The authority for this action is the Endangered Species Act of 1973 (16 U.S.C. 1531 *et seq.*).

Dated: December 19, 2006.

Cynthia K. Dohner,

Acting Regional Director, Southeast Region.

[FR Doc. E7–4367 Filed 3–9–07; 8:45 am]

BILLING CODE 4310–55–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

Buck Island, Green Cay, and Sandy Point National Wildlife Refuges in the U.S. Virgin Islands

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of intent to prepare a comprehensive conservation plan and environmental assessment; request for comments.

SUMMARY: We, the Fish and Wildlife Service, intend to gather information necessary to prepare a comprehensive conservation plan and associated environmental documents for Buck Island, Green Cay, and Sandy Point