additional properties have been determined suitable or unsuitable this week.

Dated: January 8, 2004.

**John D. Garrity,**

*Director, Office of Special Needs Assistance Programs.*

[FR Doc. 04–729 Filed 1–15–04; 8:45 am]

BILLING CODE 4210–29–M

## DEPARTMENT OF THE INTERIOR

### Office of the Secretary

### Privacy Act of 1974, as Amended; Amendment of an Existing System of Records

**AGENCY:** Department of the Interior.

**ACTION:** Proposed amendment of an existing system of records.

**SUMMARY:** The Department of the Interior (DOI) is issuing public notice of its intent to amend a Privacy Act (PA) system of records in its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a). Interior/OS–01, "Computerized ID Security System" is being amended because DOI, Office of the Secretary, National Business Center, is replacing its current computerized access control system with a new "Smart Card" access control system. The current access control system is used to maintain access control to the Main Interior complex in Washington, DC. The new access control system will be used to maintain access control to all DOI facilities that have installed smart card access control systems. In addition to the information collected under the current access control system, the new access control system will record the entry/exit locations, access status, and personal identification numbers (PIN) of the smart card holder. Two new routine uses have been added to the system of records to allow DOI to disclose information to both: (1) other agencies that have similar smart card access control systems, when a DOI smart card holder desires access to that agency's facility; and (2) to an official of another Federal agency to provide information needed by that agency in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected or maintained. Additionally, the text and/or scope of the five original routine uses have been modified to varying degrees. The data will be stored on a server located in the Main Interior building in Washington, DC, with a backup server located in the DOI National Business Center facility in Denver, CO. Data exchanged between the servers and between the servers and the client PCs will be encrypted.

**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, Mail Stop (MS)–1414-Main Interior Building (MIB), 1849 C Street, 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, 1849 C St., NW, Washington, DC 20240 (*David_A_Vanderweele@nbc.gov*).

A copy of the system notice for OS–01, Computerized ID Security System, follows.

Dated: January 12, 2004.

**Sue Ellen Sloca,**

*Office of the Secretary Privacy Act Officer, Department of the Interior.*

### Interior Department—Privacy Act Notice

#### INTERIOR/OS–01

**SYSTEM NAME:**

Computerized ID Security System—Interior, OS–01.

**SYSTEM LOCATION:**

(1) Data covered by this system are maintained in the following locations: U.S. Department of the Interior, Office of the Secretary, National Business Center, Computer Center, 1849 C Street, NW, Washington, DC 20240; 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) Limited access to data covered by this system is available at Department of the Interior (DOI) locations, both Federal buildings

and Federally-leased space, where staffed guard stations have been established in facilities that have installed the smart card ID system, as well as the physical security office(s) of those locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All individuals who have had access to DOI facilities that have the smart card access control system installed. These include, but are not limited to, the following groups: current agency employees, former agency employees, agency contractors, persons authorized to perform or use services provided in DOI facilities (e.g., Department of the Interior Federal Credit Union, Interior Department Recreation Association Fitness Center, etc.), other Government employees from agencies with smart card systems, volunteers, and visitors.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained on current agency employees, former agency employees, and agency contractors include the following data fields: Name, Social Security number, date of birth, signature, image (photograph), hair color, eye color, height, weight, organization/office of assignment, telephone number of emergency contact (optional/voluntary data field), date of entry, time of entry, location of entry, time of exit, location of exit, security access category, access status, personal identification number (PIN), number of ID security cards issued, ID security card issue date, ID security card expiration date, and ID security card serial number. Records maintained on all other individuals covered by the system include the following data fields: Name, Social Security number (or one of the following: Driver's License number, "Green Card" number, Visa number, or other ID number), 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, access status, PIN, number of ID security cards issued, ID security card issue date, ID security card expiration date, and ID security card serial number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 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 track and control ID security cards issued to persons entering and exiting the facilities.

Disclosures outside the DOI 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 smart card system when a person with a smart card desires access to that agency's facilities.

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

(i) The Department of Justice (DOJ);

(ii) a court, adjudicative or other administrative body;

(iii) a party in litigation before a court or adjudicative or 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 DOI employee acting in his or her official capacity;

(C) 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;

(D) 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 purposes for which the records were compiled.

(5) To a congressional office in response to an inquiry an individual covered by the system has made to the congressional office about him or herself.

(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.

**Note:** Disclosures within DOI of data pertaining to date and time of entry and exit of an agency employee working in the District of Columbia may not be made to supervisors, managers or any other persons (other than the individual to whom the information applies) to verify employee time and attendance record for personnel actions because 5 U.S.C. 6106 prohibits Federal Executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule program under 5 U.S.C. 6120 *et seq.*

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), 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.

ACCESS SAFEGUARDS:

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.

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:

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

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.60.)

RECORDS ACCESS PROCEDURES:

An individual requesting access to records maintained on himself or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.63.)

CONTESTING RECORD PROCEDURES:

An individual requesting amendment of a record maintained on himself or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.71.)

RECORD SOURCE CATEGORIES:

Individuals covered by the system, supervisors, and designated approving officials.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 04–939 Filed 1–15–04; 8:45 am]
BILLING CODE 4310–94–P

## DEPARTMENT OF THE INTERIOR

### Fish and Wildlife Service

### Draft Endangered Karst Invertebrate and Karst Feature Survey Guidance

**AGENCY:** Fish and Wildlife Service, Interior.

**ACTION:** Notice.

**SUMMARY:** The U.S. Fish and Wildlife Service (Service) is updating the schedule to revise and make available for public comment draft endangered karst invertebrate and karst feature survey guidance. This document is intended for use in central Texas in surveying karst features for suitable karst invertebrate habitat and to determine the presence or absence of karst invertebrates listed as endangered under the Endangered Species Act of 1973 (as amended).

**DATES:** We intend to publish a Notice of Availability for public review of the documents by March 31, 2004.

**ADDRESSES:** Field Supervisor, U.S. Fish and Wildlife Service, Austin Ecological Services Field Office, 10711 Burnet Road, Suite 200, Austin, Texas 78758; telephone (512) 490–0057; facsimile (512) 490–0974.

**FOR FURTHER INFORMATION CONTACT:** Field Supervisor, Austin Ecological Services Field Office (*see* **ADDRESSES**).

**SUPPLEMENTARY INFORMATION:**

#### Background

Sixteen invertebrate species known to occur in Bexar, Williamson, and Travis Counties, Texas, are listed as endangered under the Endangered Species Act. These invertebrates are only capable of surviving in caves or karstic rock. Karst ecosystems receive nutrients from the surface community in the form of leaf litter and other organic debris that are washed into or fall into the cave, from tree and other vascular plant roots, and/or through the feces, eggs or dead bodies of animals. In addition to providing nutrients to the karst ecosystem, the plant community also filters contaminants and buffers against changes in temperature and humidity. The major threats to karst invertebrates include the loss of habitat due to urbanization; contamination; predation by and competition with nonnative fire ants; and vandalism.

On February 27, 2003, we provided notice (68 FR 9094) of our intention to do the following:

(1) With respect to survey guidance for use in determining the presence of karst features that may contain potential habitat for endangered karst invertebrates in central Texas, we committed to work with the Texas Commission on Environmental Quality (TCEQ) and other partners to update as needed the existing TCEQ guidance on karst feature surveys.

(2) With respect to survey guidance for endangered karst invertebrates, we committed to request a panel of experts to review all new information regarding how to survey for karst invertebrates. We will use the panel's recommendations to modify the section 10(a)(1)(A) permitting requirements and to develop karst invertebrate survey guidance. This guidance was initially intended to be made available for public review and comment through a Notice of Availability to be published in the **Federal Register** by December 30, 2003.

We submitted both draft guidance documents to a panel of 48 individuals with expertise and interest in conservation of karst invertebrates. The panel met with us on September 8, 2003, and individuals on the panel provided feedback on both guidance documents. We are incorporating comments and suggestions provided by the panel into the guidance for surveying for the presence or absence of karst invertebrates. We will resubmit this updated document to the karst panel for additional review and comment. As a result, the notice of availability for public review of this document will be delayed. We now intend to publish the notice by March 31, 2004.

**Authority:** The authority for this action is the Endangered Species Act, as amended (16 U.S.C. 1532 *et seq.*).

Dated: November 28, 2003.

**R. M. McDonald,**

*Acting Regional Director.*

[FR Doc. 04–964 Filed 1–15–04; 8:45 am]
BILLING CODE 4310–55–P

## DEPARTMENT OF THE INTERIOR

### Bureau of Indian Affairs

### Indian Gaming

**AGENCY:** Bureau of Indian Affairs, Interior.

**ACTION:** Notice of approved Class III Gaming Compact.

**SUMMARY:** This notice publishes the approval of the Class III Gaming Compact between the State of New Mexico and the Navajo Nation. Under the Indian Gaming Regulatory Act of 1988, the Secretary of the Interior is required to publish notice in the **Federal Register** approved Tribal-State compacts for the purpose of engaging in Class III gaming activities on Indian lands.

**EFFECTIVE DATE:** January 16, 2004.

**FOR FURTHER INFORMATION CONTACT:** George T. Skibine, Director, Office of Indian Gaming Management, Office of the Deputy Assistant Secretary—Policy and Economic Development, Washington, DC 20240, (202) 219–4066.