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 authorized to access them, (3) to ensure that persons signing official documents are indeed the person 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.

Disclosures outside the DOI may be made:

(a) 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.

(b) 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.

(c) To another agency with a similar smart card system when a person with a DOI SmartCard desires access to that other agency's facility.

(d) To the Department of Justice, or to a court, adjudicative or other administrative body, or to a party in litigation before a court or adjudicative or administrative body, when:

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

(i) The Department or any component of the Department;

(ii) Any Departmental employee acting in his or her official capacity; or

(iii) Any Departmental employee acting in his or her individual capacity where the Department or the Department of Justice has agreed to represent the employee; and

(2) We deem the disclosure to be:

(i) Relevant and necessary to the proceeding; and

(ii) Compatible with the purpose for which we compiled the information.

(e) To the appropriate Federal agency that is responsible for investigating, prosecuting, enforcing or implementing a statute, rule, regulation or order, when we become aware of an indication of a violation or potential violation of the statute, rule, regulation, or order.

(f) To a congressional office in response to a written inquiry to that office by the individual to whom the record pertains.

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, magnetic tapes.

RETRIEVABILITY:

Records are retrievable from EACS by name, digital certificate and personal identification number (PIN), and Web home address.

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. EACS access granted to individuals is password-protected. Access to the certificate issuance portion of this system of records is controlled by a digital certificate in combination with a PIN. Each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when first displayed. 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 safeguard requirements are met.

RETENTION AND DISPOSAL:

Records relating to persons covered by this system are retained in accordance with General Records Schedule.

SYSTEM MANAGER(S) AND ADDRESS:

Office of the Chief Information Officer, Office of the Secretary, Department of the Interior, 625 Herndon Parkway, Herndon, VA 20170.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on him or herself should address his/her request to the local Bureau/office IT computer administrators or help desk. Individuals requesting notification must provide their full name and social security number. Interior bureaus/offices are listed at the Department of the Interior Web site at *http://www.doi.gov*. 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 him or herself should address his/her request to the office listed in the ''Notification procedures'' section above. Individuals requesting access must provide their full name and social security number. 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 him or herself should address his/her request to the office above. Individuals requesting an amendment must provide their full name and social security number. The request must be in writing and signed by the requester. (*See* 43 CFR 2.71).

RECORD SOURCE CATEGORIES:

Information in this system is obtained from individuals covered by the system supervisors, designated approving officials, certificate issuing authority, and network system administrators.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 05–289 Filed 1–5–05; 8:45 am]

BILLING CODE 4310–RK–P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

Privacy Act of 1974, as Amended; Addition of a New System of Records

AGENCY: U.S. Department of the Interior.

ACTION: Proposed addition of a new system of records.

SUMMARY: The Department of the Interior (DOI) is issuing public notice of its intent to create 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). This action is necessary to meet the requirements of the Privacy Act to publish in the **Federal Register** notice of the existence and character of records systems maintained by the agency (5 U.S.C. 552a(e)(4)). The new system of records is captioned, ''Interior—DOI–15,'' and is titled, ''Authenticated Computer Access and Signature System (ACASS).''

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 Department of the Interior, Privacy Act Officer, Marilyn Legnini, U.S. Department of the Interior, Mail Stop (MS)–5312—Main

Interior Building (MIB), 1849 C Street, NW., Washington, DC 20240. 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: Bob Donelson, Senior Property Manager, Bureau of Land Management, Department of the Interior, 1620 L Street, NW., MS LS, Washington, DC 20036; 202–452–5190.

SUPPLEMENTARY INFORMATION: The primary purpose of ACASS is: (1) To ensure the security of DOI computer networks in order to maintain continuous communications and protect the information attached to the networks from unauthorized access, tampering or destruction; (2) To verify that all persons accessing DOI networks with ''smart card'' systems are authorized to access them; (3) To ensure that persons signing official documents are indeed the person represented and to provide assurance to the recipient that the signature is authentic; and (4) To enable an individual to encrypt and decrypt documents for secure transmission.

The new ''smart card'' access control system is based on digitally encrypted certificates. The DOI is adding the capability for users to electronically sign documents and encrypt documents using digital certificates. The current password access control system is used to maintain access control to the various computer networks and computer systems in the DOI. The new access control system will be used to maintain access control to all DOI computer networks and systems that have installed ''smart card'' access controls. In addition to the information collected under the current access control system, the new access control system will record the personal identification numbers (PIN) of the ''smart card'' holder onto the ''smart card''. The PIN will not be recorded elsewhere in the system. The data will be stored on a server located in the U.S. Department of the Interior, Bureau of Land Management, National Information Resources Management Center, Denver Federal Center, Lakewood, Colorado. A redundant, fail-over, server is located at BLM's Network Operations Center in Portland, Oregon.

A copy of the system notice for Interior—DOI–15, Authenticated Computer Access and Signature System (ACASS), follows.

Dated: January 3, 2005.

Marilyn Legnini,

Departmental Privacy Act Officer, Department of the Interior.

INTERIOR/DOI–15

SYSTEM NAME:

Authenticated Computer Access and Signature System—Interior, DOI–15

SYSTEM LOCATION:

(1) Data covered by this system are maintained in the following locations: U.S. Department of the Interior (DOI), Bureau of Land Management (BLM), National Information Resources Management Center, Denver Federal Center, Lakewood, Colorado. A redundant, fail-over, server is located at BLM's Network Operations Center in Portland, Oregon. A repository of digital certificates included in this system is maintained by the certificate authority. However, only the Department of Interior maintains a listing of individuals to whom the certificates are issued.

(2) Limited access to data covered by this system is available at DOI locations, both Federal buildings and Federally-leased space, where DOI computer systems are located. System Administrators at those locations have access only to the information for employees who attempt to access computer systems at their location.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All individuals who have ''smart card'' IDs with authentication capability who are granted access to DOI computer networks or certain isolated systems at facilities that have the ''smart card'' access control system installed and individuals authorized to sign official DOI documents. These include, but are not limited to, the following groups: current agency employees, former agency employees until the records are disposed of in accordance with the proscribed records schedule, agency contractors, other Government employees from agencies with ''smart card'' systems and volunteers.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained on current agency employees and agency contractors include the following data fields: Name, organization/office of assignment, 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. The Active Directory is a component of the computer network operating system used by DOI that performs network management functions and is the repository for the computer access data. A contracted certification authority provides the digital certificates and encryption services necessary for secure authentication and verification. The collected data will contain the individual's user ID/e-mail address. The Active Directory will generate the date of entry to the computer network/system, time of entry, location of entry, time of exit, security access category, and access status which will also become part of the record. The collected data retained in Active Directory may also contain: office telephone number, supervisor's name and Web home page address. Records on former agency employees are maintained in accordance with the proscribed records schedule.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

Federal Information Security Act (Pub.L. 104–106), section 5113.

E-Government Act (Pub.L. 104–347), section 203.

Government Paperwork Elimination Act (Pub.L. 105–277).

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 security of DOI computer networks to maintain continuous communications and protect the information attached to the networks from unauthorized access, tampering or destruction.

(2) To verify that all persons accessing DOI networks with ''smart card'' systems are authorized to access them.

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

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

DISCLOSURES OF RECORDS WITHIN DOI:

Disclosure of these records may be made: (1) To those officers and employees of DOI who have a need for the record in the performance of their duties, or (2) when required by the Freedom of Information Act, 5 U.S.C. 552.

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 another agency with a similar ''smart card'' system when a person with a ''smart card'' requires access to that agency's facilities on a ''need-to-know'' basis.

(3) To the Federal Protective Service and appropriate Federal, State, or local 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.

(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 a written 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 National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2903 and 2904.

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, magnetic tapes and the ID authentication card itself and on paper records stored in file cabinets in secured locations.

RETRIEVABILITY:

Records are retrievable from Active Directory by organization, agency point of contact, security access category that describes the type of access the user is allowed, date of system 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. Active Directory access granted to individuals is password-protected. Access to the certificate issuance portion of this system of records is controlled by a digital certificate in combination with a personal identification number (PIN). Each person granted access to the system 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. Backup tapes are stored in a locked and controlled room in a secure, off-site location. A Privacy Impact Assessment was used to ensure that Privacy Act requirements and safeguard requirements were 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 the ID security card expiration date.

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

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

SYSTEM MANAGER(S) AND ADDRESS:

Director, Information Resources Management Center, Bureau of Land Management, Denver Federal Center, Building 40, P.O. Box 25047, Denver, Colorado 80225–0047.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should address his/her request to the local office Information Technology Security Manager. The individual requesting notification must provide their full name and social security number. Interior bureaus/offices are listed at the Department of the Interior Web site at *http://www.doi.gov.* 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 local office Information Technology Security Manager. The individual requesting access must provide their full name and social security number. 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 local office IT Security Manager. The individual requesting the amendment must provide their full name and social security number. 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, certificate issuing authority, network system administrators.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 05–292 Filed 1–5–05; 8:45 am]

BILLING CODE 4310–RK–P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

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

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Proposed amendment of an existing system of records.

SUMMARY: Under the Privacy Act of 1974, as amended (5 U.S.C. 552a), the Office of the Secretary is issuing public notice of our intent to change an existing Privacy Act system of records notice entitled, Interior BIA–18 ''Law