

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 of 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.

(13) To the Office of Management and Budget during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

(14) To the Department of the Treasury to recover debts owed to the United States.

(15) To the news media when the disclosure is compatible with the purpose for which the records were compiled.

DISCLOSURES TO CONSUMER REPORTING AGENCIES:

Pursuant to 5 U.S.C. 552a(b)(12), records can be disclosed to consumer reporting agencies as they are defined by the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

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

STORAGE:

Records are stored in both manual and electronic format. Manual records are maintained in letter files, application files, and computer printouts. Electronic records are maintained in network access storage, on hard disks, and on magnetic tapes.

RETRIEVABILITY:

Records are:

(a) Indexed by name of borrower, loan guaranty number, and tribal name when applicable.

(b) Retrieved by manual search or computer inquiry.

SAFEGUARDS:

LOMAS is maintained with controls meeting safeguard requirements identified in Departmental Privacy Act Regulations (43 CFR 2.51) for manual and automated records. Access to records is limited to authorized personnel whose official duties require such access; agency officials have access only to records pertaining to their agencies.

(1) Physical Security: Paper or electronic format records are maintained

in locked file cabinets and/or in secured rooms.

(2) Technical Security: Electronic records are maintained in conformity with Office of Management and Budget and Departmental guidelines reflecting the implementation of the Federal Information Security Management Act. Electronic data is protected through user identification, passwords, database permissions, and software controls. These security measures establish different degrees of access for different types of users. An audit trail is maintained and reviewed periodically to identify unauthorized access. A Privacy Impact Assessment was completed for LOMAS and is updated at least annually to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met.

(3) Administrative Security: All DOI and contractor employees with access to LOMAS are required to complete Privacy Act, Records Management Act, and Security Training.

RETENTION AND DISPOSAL:

Records relating to individuals covered by this system are retained in accordance with the 16 Bureau of Indian Affairs Manual (BIAM), as approved by the National Archives and Records Administration (NARA), and are scheduled for permanent retention. All records of guaranteed or insured loans are stored permanently. Records of loans that are paid, cancelled, or otherwise disposed of are archived. Records of rejected loans are stored for 1 year and then archived.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Indian Energy and Economic Development, Office of the Assistant Secretary—Indian Affairs, 1951 Constitution Avenue, NW., MS SIB-20, Washington, DC 20245.

NOTIFICATION PROCEDURES:

Inquiries regarding the existence of records should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the requirements of 43 CFR 2.60.

RECORDS ACCESS PROCEDURES:

A request for access may be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the requirements of 43 CFR 2.63.

CONTESTING RECORD PROCEDURES:

A petition for amendment should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the content requirements of 43 CFR 2.71.

RECORD SOURCE CATEGORIES:

Information is received from individuals on whom the records are maintained, commercial banks, BIA employees and contractors, and purchasers of guaranteed or insured loans.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8-16098 Filed 7-14-08; 8:45 am]

BILLING CODE 4312-RY-P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

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

AGENCY: Bureau of Indian Affairs.

ACTION: Notice of addition of a new system of records.

SUMMARY: The Department of the Interior (DOI), Bureau of Indian Affairs is issuing public notice of its intent to add a new Privacy Act system of records to 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)). This new Privacy Act system of records is entitled Interior, BIA-31: "Information Management System" (IMS).

DATE: Comments must be received by August 25, 2008.

ADDRESSES: Any persons interested in commenting on this new system of records may do so by submitting comments in writing to the Privacy Act Officer, 625 Herndon Parkway, Herndon, VA 20170, or by e-mail to *Joan.Tyler@bia.gov*.

FOR FURTHER INFORMATION CONTACT:

Nicole Jaber, Director, Division of Internal Validation and Verification, Office of the Chief Information Officer, 625 Herndon Parkway, Herndon, VA 20170, or by e-mail at *Nicole.Jaber@bia.gov*.

SUPPLEMENTARY INFORMATION: This notice is published pursuant to the Privacy Act of 1974 (5 U.S.C. 552a(3)(4)) and is in exercise of authority delegated by the Secretary of the Interior to the Assistant Secretary—Indian Affairs in 209 DM 8.1. This notice establishes the Privacy Act system or record entitled Interior, BIA-31, "Information Management System" (IMS).

The purpose of IMS is to automate the management of all types of documents

in a single database. Records in the system are maintained as electronic copies only. IMS provides a Web-based document management system accessible via a browser interface with the Office of the Assistant Secretary of Indian Affairs, and the Bureau of Indian Affairs. Documents are stored in the database in any file format, such as, but not limited to, Microsoft Word, Excel, Power Point, and scanned PDF or TIF files. Documents can be routed from one person to another for assignment, comment, response, editing, surname, and signature. A variety of status reports are available to track the progress of workflows. Routing includes communication tools for route members to add comments to the workflow. Documents can be electronically delivered to a number of individuals simultaneously, either for a response or for read only purposes.

Dated: July 9, 2008.

George T. Skibine,

Acting Deputy Assistant Secretary, Policy and Economic Development.

SYSTEM NAME:

Information Management System (IMS); Interior, BIA-31.

SYSTEM LOCATION:

Herndon Data Center (HDC), 625 Herndon Parkway, Herndon, VA 20170.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are employees of BIA and AS-IA who are the originators or approving officials for government documentation.

CATEGORIES OF RECORDS IN THE SYSTEM:

- (1) Information about employees to include name, work location and home address, work and home telephone number and fax numbers;
- (2) Employee's office information, title, supervisor, and supervisory status;
- (3) AS-IA and BIA Offices;
- (4) Documents generated, their originator and originating office, and their approval destination(s); and
- (5) Document tracking data and document suspense requirements.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system of records is maintained under the authority of 25 U.S.C. 1, 1a, 13; 18 U.S.C. 3055; 25 U.S.C. 480.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The system is used to manage all AS-IA correspondence in a single database. IMS contains information to facilitate the efficiency of the correspondence process throughout AS-IA. The system

will allow the tracking of correspondence from receipt to completion/response, provide valuable information to AS-IA coordinators, identify duplicate requests, ensure consistency in responses, reduce processing time, support action on correspondence, and improve customer service. IMS facilitates the management of documents, maintains multiple versions of any single document, and provides a mechanism to distribute documents to a group of individuals with the capability for the group members to respond/reply to the sender, and to manage/track workflow.

Disclosure(s) outside the Department of the Interior may be made:

(1)(a) To any of the following entities or individuals, when the circumstances set forth in paragraph (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 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 purposes for which the records were compiled.

(2) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if covered individual is deceased, has made to the office.

(3) To any criminal, civil, or regulatory law enforcement authority (whether Federal, State, territorial, local, tribal, or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature, and the

disclosure is compatible with the purpose for which the records were compiled.

(4) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(5) To Federal, State, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing, or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant, or other benefit, when the disclosure is compatible with the purpose of which the records were compiled.

(6) To representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

(7) To State and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

(8) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

(9) The 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 of 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.

(10) To the Office of Management and Budget during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

(11) To the Department of the Treasury to recover debts owed to the United States.

(12) To the news media when the disclosure is compatible with the purpose for which the records were compiled.

DISCLOSURES TO CONSUMER REPORTING AGENCIES:

Pursuant to 5 U.S.C. 552a(b)(12), records can be disclosed to consumer reporting agencies as they are defined by the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

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

STORAGE:

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

RETRIEVABILITY:

Users can access the IMS system by navigating (via browser) to the IMS logon Web page, and successfully entering their login credentials. Documents stored in IMS are retrieved by document name, subject matter, or author.

SAFEGUARDS:

IMS is maintained with controls meeting safeguard requirements identified in Departmental Privacy Act Regulations (43 CFR 2.51) for manual and automated records. Access to records is limited to authorized personnel whose official duties require such access; agency officials have access only to records pertaining to their agencies.

(1) Physical Security: Electronic format records are maintained in locked file cabinets and/or in secured rooms. Buildings have security guards and/or secured doors, and all entrances are monitored by electronic surveillance equipment on a 24/7 basis.

(2) Technical Security: Electronic records are maintained in conformity with Office of Management and Budget and Departmental guidelines reflecting the implementation of the Federal Information Security Management Act. Electronic data are protected through user identification, passwords, database permissions, and software controls. These security measures establish different degrees of access for different types of users. An audit trail is maintained and reviewed periodically to identify changes made to records. A Privacy Impact Assessment was completed for the IMS and is updated at least annually to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met.

(3) Administrative Security: All DOI and contractor employees with access to IMS are required to complete Privacy Act, Records Management Act, and Security Awareness Training.

RETENTION AND DISPOSAL:

Records relating to individuals covered by this system are retained in accordance with the 16 Bureau of Indian Affairs Manual (BIAM), approved by the National Archives and Records Administration (NARA), and scheduled for permanent retention.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Information Operations (OIO), Office of the Chief Information Officer, 625 Herndon Parkway, Herndon, VA 20170.

NOTIFICATION PROCEDURES:

Inquiries regarding the existence of records should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the requirements of 43 CFR 2.60.

RECORDS ACCESS PROCEDURES:

A request for access should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the requirements of 43 CFR 2.63.

CONTESTING RECORD PROCEDURES:

A petition for amendment should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the content requirements of 43 CFR 2.71.

RECORD SOURCE CATEGORIES:

Authorized user data comes from the Identity Information System (IIS). The subject document data is entered by the user.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8-16099 Filed 7-14-08; 8:45 am]

BILLING CODE 4312-RY-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: The Department of the Interior (DOI), Bureau of Indian Affairs (BIA) is issuing public notice, pursuant to the Privacy Act of 1974 (5 U.S.C.

552a), of its intent to amend its existing Privacy Act system of records notice entitled Interior, BIA-07, "Tribal Rolls," published at 48 FR 41098 (September 13, 1983).

DATES: Comments must be received by August 25, 2008.

ADDRESSES: Any persons interested in commenting on this proposed amendment may do so by submitting comments in writing to the Privacy Act Officer, Bureau of Indian Affairs, 625 Herndon Parkway, Herndon, VA 20170, or by e-mail to Joan.Tyler@bia.gov.

FOR FURTHER INFORMATION CONTACT: Dolores Ayotte, Acting Superintendent, Alaska Region, West Central Alaska Agency, Bureau of Indian Affairs, Department of the Interior, 3601 C Street, Suite 1100, Anchorage, AK 99503, or by e-mail to Delores.Ayotte@bia.gov.

SUPPLEMENTARY INFORMATION: This notice is published pursuant to the Privacy Act of 1974 (5 U.S.C. 552a(e)(4)) and is in exercise of authority delegated by the Secretary of the Interior to the Assistant Secretary—Indian Affairs in 209 DM 8.1. This notice amends the Privacy Act System of Records entitled Interior, BIA-07, "Tribal Rolls."

The purpose of this amendment is to: (1) Change the name of the system to Interior, BIA-07, "Progeny;" (2) update the information on the location of the records and the technology used to store and retrieve records; (3) more clearly state the information that is included in the system of records; (4) more clearly state the current routine uses of the records by organizations and individuals outside of the Department of the Interior; and (5) expand the routine uses of such information to include using these records as a basis for the creation of the Certificate of Degree of Indian Blood (CDIB) for the Alaska Native Claims Settlement Act (ANCSA) enrollees and descendants. A copy of the notice, with changes incorporated, is attached.

Dated: July 9, 2008.

George T. Skibine,
Acting Deputy Assistant Secretary, Policy and Economic Development.

SYSTEM NAME:

Progeny—Interior, BIA-07.

SYSTEM LOCATION:

(1) BIA Albuquerque Data Center, 1011 Indian School Rd. NW., Albuquerque, NM 87104.

(2) Other BIA Area, Agency, and Field Offices. (For a listing of specific locations, contact the System Manager.)