including grades, attendance records, health, special programs, and behavior information are stored in paper form in locked file cabinets. Electronic records are stored on hard disks.

**RETRIEVABILITY:**

Records including attendance, grades, discipline information, test and assessment histories, program enrollments, and health information are retrieved from the NASIS using a unique student identification code assigned by the system. Other records for school administrators, principals, teachers, teacher aides, counselors, school bus drivers, line officers, regional directors, system administrators, librarians, food service workers, dormitory managers, and parents/guardian records are retrievable using a unique identifier code assigned by the system for each individual.

**SAFEGUARDS:**

NASIS 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 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 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 unauthorized access. A Privacy Impact Assessment was completed for the NASIS and is updated at least annually to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met. Security procedures are verified through annual assessments of the applications. The NASIS Security Assessment was last performed 12/19/2006 in accordance with FIPS 200 and NIST 800–53.

(3) *Administrative Security:* All DOI and contractor employees with access to NASIS 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), as approved by the National Archives and Records Administration (NARA), and are scheduled for permanent retention.

**SYSTEM MANAGER(S) AND ADDRESS:**

NASIS COTR and Project Manager, Bureau of Indian Education, 1001 Indian School Road, NW, Suite 219A, Albuquerque, NM 87103

**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 students attending BIE-funded schools, parents/guardians of students, school administrators, principals, teachers, teacher aides, counselors, school bus drivers, librarians, food service workers, and dormitory managers on whom records are maintained.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

[FR Doc. E8–16103 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, Interior.

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

**SUMMARY:** The Department of the Interior, Bureau of Indian Affairs (BIA) 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. 552). 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 Privacy Act system of records is entitled Interior, BIA–30, ''Identity Information System'' (IIS).

**DATES:** 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 Independent 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(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 establishes the Privacy Act system of records entitled Interior, BIA–30, ''Identity Information System'' (IIS). The purpose of this system is to provide an automated tool to track the security screening of BIA and Assistant Secretary—Indian Affairs (AS–IA) employees and contractors. It enables or allows BIA and AS–IA to record completion of official required IT security training and track requests for access to BIA IT information systems.

Dated: July 9, 2008.

**George T. Skibine,**

*Acting Deputy Assistant Secretary, Policy and Economic Development.*

**SYSTEM NAME:**

Identity Information System (IIS)—Interior, BIA–30.

**SYSTEM LOCATION:**

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

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Those members from the following organizations who require access to BIA IT systems:

(1) Employees and contractors of AS–IA, BIA and the Bureau of Indian Education (BIE)

(2) Office of the Special Trustee for American Indians (OST)

(3) Office of Hearings and Appeals (OHA)

(4) Office of Historical Trust Accounting (OHTA)

(5) Bureau of Land Management (BLM)

(6) Tribal users covered under a 638 Compact/Contract

**CATEGORIES OF RECORDS IN THE SYSTEM:**

(1) Individual data including the name, title, birth date, Social Security Number, phone number, office name, and office location;

(2) Agency affiliation and status as employee or contractor

(3) Status of required training;

(4) System role based accesses granted to each user;

(5) Building access badge information;

(6) Acceptance date of BIA Rules of Behavior;

(7) Record showing that background status has been confirmed by personnel security;

(8) IT systems for which access has been requested and the status of those requests;

(9) Supervisor or government approver records showing those users whose access or removal request needs to be approved by the supervisor or government approver;

(10) Business owner records showing those users whose access or removal request needs to be approved by the business owner;

(11) System administrator records showing the names of those users whose access needs to be set up or revoked;

(12) Contract Officer Technical Representative (COTR) records showing the names and other data of contract IT users employed on a contract under the administrative support of that COTR.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

This system of records is maintained under the authority of 25 U.S.C. 1, 1a, 13; 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 record and manage contact, training, and security screening information about BIA and AS–IA employees and contractors; and to manage access by BIA and AS–IA employees and contractors to BIA information systems.

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 for 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 on network storage devices, (*e.g.*, hard disks, magnetic tapes) and on paper.

**RETRIEVABILITY:**

IIS users view their own data by signing onto IIS with their user name and password. Additional access to data

is role based. For example, supervisors and COTRs can see the data of those for whom they are responsible, and IIS system administrators can see the data for all users in the system.

**SAFEGUARDS:**

IIS 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 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 unauthorized access. A Privacy Impact Assessment was completed for the IIS 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 IIS 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), as approved by the National Archives and Records Administration, 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 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:**

Individuals on whom the records are maintained providing information on themselves, managers issuing approvals for system access requests, IT technicians reporting status of IT system access requests, and personnel security officers reporting verification of background investigations.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

[FR Doc. E8–16104 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; Addition of a New System of Records

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

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

**SUMMARY:** The Department of the Interior (DOI), Bureau of Indian Affairs (BIA) 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)). The new Privacy Act system of records is entitled Interior, BIA–29: ''Fee to Trust Tracking System'' (FTTS).

**DATE:** 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:** Vicki Forrest, Deputy Bureau Director, Office of Trust Services, 1849 C Street, NW., Washington, DC 20240, or by e-mail at *Vicki.Forrest@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 Principal Deputy Assistant Secretary—Indian Affairs in 209 DM 8.1. This notice establishes the Privacy Act system of records entitled Interior, BIA–29: ''Fee to Trust Tracking System'' (FTTS).

FTTS was developed for the BIA to track applications for conversions of land from fee ownership into trust status for Tribes and individual Indians. FTTS is replacing an existing legacy system, Fee to Trust (FTT), that does not collect sufficient information to properly track applications.

Dated: July 9, 2008.

**George T. Skibine,**

*Acting Deputy Assistant Secretary for Policy and Economic Development—Indian Affairs.*

**SYSTEM NAME:**

Fee to Trust Tracking System (FTTS), Interior, BIA–29.

**SYSTEM LOCATION:**

Office of Information Operations, Bureau of Indian Affairs, 625 Herndon Parkway, Herndon, VA 20170.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

(1) Individuals applying to the Department of the Interior (DOI) for conversion of land from fee ownership into trust status.

(2) Individuals, Tribes, organizations or other stakeholders or their representatives with an interest in applications for converting land from fee ownership into trust status.

(3) DOI employees or contractors who process the applications for conversion of land from fee ownership into trust status if their contact information is required.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

(1) Statistical information necessary to improve and streamline the process, as well as, budget preparatory information to support the entire transfer of fee simple land into trust lands for tribes and individual Indians.

(2) Information required by the trust fee lands transfer case packet application, including but not limited to, a legal description of the trust fee land packet, and the name, phone number and address of the party (or parties) filing the application.

(3) Legal representation information pertaining to the trust fee lands transfer packet application, including but not