U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Native American Student Information System (NASIS)
Bureau/Office: Bureau of Indian Education, Office of Indian Education Programs
Date: January 8, 2021
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Native American Student Information System (NASIS) is a commercial-off-the-shelf, "contractor-owned, contractor-operated (COCO)," major application that provides the Bureau of Indian Education (BIE) a centralized system for supporting teachers, principals, students, parents, Education Resource Center (ERC) staffs, and the Central Office staff. The purpose of NASIS is to ensure relevant data is collected for the BIE and is available for school improvement planning, to improve student achievement, and to meet regulatory and statutory reporting requirements. It generates statistical reports required to meet federal requirements and source data to analyze student performance. NASIS allows access to data and reports at schools, ERCs, the Regional Director and Central Office levels.

The other function of NASIS is the delivery of student and school services that are similar to those present in most school systems. NASIS provides schools with the support needed to satisfy day-to-day operations and instructional planning needs. This includes data input, collection, and reporting for a variety of functions such as, but not limited to, scheduling, attendance, grades, behavior tracking, test and assessment histories, program enrollments, health information, and other areas of need.

The requirement for a BIE information system originated in the Educational Amendments of 1978 to Pub. L. 95-561 amended in 2001 as the "Native American Education Improvement Act." NASIS is intended to meet current reporting requirements of the Elementary and Secondary Education Act of 1965 [As Amended through Pub. L. 116–94, Enacted December 20, 2019] and the Individuals with Disabilities Education Act, Pub. L. 94-142, as amended by Pub. L. 105-17, Part B, Section 611(a) (1). NASIS supports the fulfillment of these statutes and the maintenance of the Indian School Equalization Program (ISEP) regulatory requirements.

The BIE oversees a total of 183 elementary, secondary, residential and peripheral dormitories across 23 states; 130 schools are tribally controlled under Pub. L. 93-638 contracts or Pub. L. 100-297 Tribally Controlled Grant Schools Act, and 53 schools are operated by the BIE. The BIE elementary and secondary school system serves about 47,218 individual students with a calculated three-year Average Daily Membership of 41,027 students. The 183 schools vary considerably by size, tribal culture, and a multitude of other socio-economic and geographic factors.

This privacy impact assessment covers the current NASIS system and its replacement, NASIS 2.0. The NASIS system will remain in operation until NASIS 2.0 is fully commissioned. The BIE will then migrate current data to NASIS 2.0 from NASIS, which will then be decommissioned. When information in this PIA is specific to a NASIS application it will be identified as such, otherwise it will be identified with the acronym NASIS.

C. What is the legal authority?

25 U.S.C. 1, 1a, 13; 25 U.S.C. 480; Public Law 95-561 and subsequent amendments; 25 CFR parts 31, 32, 36, and 39; the Snyder Act (25 U.S.C. 13); Johnson-O'Malley Supplemental Indian Education Program Modernization Act (25 U.S.C. 5301); Elementary and Secondary Education Act (20 U.S.C. 6301); Tribally Controlled Schools Act (25 U.S.C. 2501 et seq.); Indian Self-Determination and Education Assistance Act, as Amended (Pub. L. 93-638; Indian Education Amendments of 1978 (25 U.S.C. 2001 et seq.); Individuals with Disabilities Education Act (IDEA) (20 U.S.C. 1400 et seq.); Elementary and Secondary Education Act of 1965 (As amended through Pub. L. 115-224, Enacted July 31, 2018).

D. Why is this PIA being completed or modified?

☒ New Information System (Applicable to NASIS 2.0)
☐ New Electronic Collection
☒ Existing Information System under Periodic Review (Applicable to NASIS)
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records

☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000000083, Native American Student Information System (NASIS) System Security and Privacy Plan

NASIS 2.0 is registered in CSAM. It is in the development stage and does not have a UII Code. However, NASIS 2.0 will replace NASIS and will use the same UII Code, as NASIS.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	Not Applicable	Not Applicable	Not Applicable

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

Records in NASIS are maintained under DOI system of records notice BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008). This SORN may be viewed at https://www.doi.gov/privacy/bia_notices. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

OMB Control Number 1076-0122, Data Elements for Student Enrollment in Bureau-funded Schools, Expires December 31, 2021

OMB Control Number 1076-0134, Student Transportation Form, Expires February 28, 2022

OMB Control Number 1076-0176, IDEIA Part B and C Child Count, Expires January 31, 2021

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Disability Information
☒ Other Names Used
☒ Employment Information
☒ Emergency Contact
☒ Mailing/Home Address
☒ Social Security Number (SSN)
☒ Race/Ethnicity
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Education Information
☒ Legal Status
☒ Place of Birth
☒ Other: Certificate of Indian Blood (Tribe), parent information, and student demographics used for student registration and placement obtained from parents.

Username and /Password are collected from individuals authorized access to NASIS for identification and authentication purposes.

The Social Security Number (SSN) is collected on school staff is used for employment background investigations and teacher credentials. SSN is currently being used to accurately identify students with the same name and date of birth, thereby ensuring accurate academic records are created and assigned to the correct student during enrollment and for grade and program placement. BIE is planning to phase out use of the SSN to be replaced by a student identification number to comply with OMB Circular A-130, Managing Federal Information as a Strategic Resource, and Departmental policy of reducing the use of SSNs to protect privacy.

Student Information. Student information including name, nick name, birth date, address, phone number, email address, NASIS ID number, student school and State ID information, student photo, school, residential enrollment, free or reduced meal status, and household census information; student tribal affiliation, tribal certificate type, and validation of tribal membership; Federal Race/Ethnicity Designation and Hispanic/Latino Race/Ethnicity Determination used for Federal reporting purposes, student contact information including contact information for parents or guardians or other parties to contact in an emergency, and relationships of students to emergency contacts; records documenting student behavior including information on behavior problems and the resolution of the problems; transcripts, test scores, grades, education level, classes available, class scheduling, special education data, gifted and talented data, instructional and residential attendance; school bus transportation data; languages spoken by students, level of English proficiency, indigenous Indian languages spoken, and preferred language; immunization records of students, health conditions of students and other information pertaining to student health, including treatments for health problems; miscellaneous demographic information such as date entered United States (U.S.), date entered U.S. school.

Parent or Guardian Information. Parents or guardians of, and emergency or authorized contacts for, students attending BIE-funded primary and secondary schools. Personally identifiable information (PII) collected consists of name, birth date, gender, personal email address, cell

phone, work phone, and household information such as household name (guardian's first and last name, phone number associated with the household, and address).

School Staff. Information on school staff who work at BIE-funded primary and secondary schools, including school administrators, principals, registrars, school clerks, teachers, teacher aides, counselors, school bus drivers (for certifications), janitorial staff, food service staff, school complex security staff, and dormitory staff. PII collected consists of name, SSN, staff ID number, state education license number (State ID), qualifications for staff position, title, school staff seniority level, number of years teaching, education level; school district of employment and school district assignments, home address, home phone number, and home email address general and emergency contact information.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☒ State agency
☒ Other: 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.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☐ Web site
☒ Fax
☒ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

D. What is the intended use of the PII collected?

The system is used to administer BIE-funded schools by providing high quality data to authorized users. NASIS serves as the BIE's primary tracking and reporting system for students attending BIE-funded schools and for duty certifications of employees at such schools. The PII collected is used for student identification to ensure accurate academic records are created and assigned during enrollment, for grade assignment and program placement, to contact a student's parent or guardian in the case of an emergency, and for other U.S. Department of Education (ED) reporting requirements.

The PII collected on school staff is used for contact information, teacher credentials, and demographics that are not reported individually, but in aggregate for reporting to ED.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII is shared with the Central Office and Division of Performance and Accountability (DPA) located in Washington, DC, and three Associate Deputy Director Offices, Educational Resource Centers (ERC) nationwide, and 184 schools and dormitories in the continental United States. PII is used to conduct analysis for school improvement planning, for instructional planning needs to improve student achievement; for student scheduling, behavior tracking, testing and assessment histories; determining program enrollment, health management, and to support day-to-day school operations; to contact a student's parent or guardian in the case of an emergency, and for other U.S. Department of Education (ED) reporting requirements.

Information may be shared with any BIE employee acting in their official capacity in the performance of official functions.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Government Accountability Office in the form of reports required under the Government Performance and Results Act (GPRA); Federal Bureau of Investigation for the purpose of reporting suspected child abuse or neglect; ED for accountability and reporting requirements; and as authorized under the Privacy Act of 1974 and the routine uses I the BIA-22, Native American Student Information System (NASIS), system of records notice, which may be viewed at: https://www.doi.gov/privacy/bia_notices.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

To State education departments in the form of data for assessment access for students and attendance and graduation rate data for students within that State for the purpose of fulfilling accountability requirements under ESSA.

To Tribal, State or Local Agencies for the purpose of reporting suspected child abuse or neglect.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with BIE contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support and as authorized pursuant to the routine uses contained in BIA-22, Native American Student Information System (NASIS) system of records notice.

☒ Other Third-Party Sources: *Describe the third-party source and how the data will be used.*

Parents and guardians of students in the form of reports pertaining to grades, assignments, attendance, behavior, schedule, and school calendar for their student. To an authorized recipient such as a parent, medical facility, service provider, or school to which the student is transferring, in the form of a data package containing information about the student to enable the recipient to provide services to the student, following the guidelines of the IDEA for special education students, or privacy policies for DOI and Family Education Rights and Privacy Act (FERPA) for all other students.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals do have the option of not providing information when completing the Student Enrollment Application for Students enrolled in Bureau-Funded Schools Form. The information collected is used to determine eligibility for attendance at Bureau-funded schools and is used to determine the level of funding to be distributed by formula to BIE-funded elementary and secondary schools. Providing the information is voluntary. Not providing the information could result in the BIE not being able to process the application and the student would not be enrolled in school.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is included on the Data Elements for Student Enrollment in Bureau-funded Schools form (OMB Control Number 1076-0122, Expires 12/31/2021).

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment and the published BIA-22, Native American Student Information System (NASIS) system of records notice, 73 FR 40605, July 15, 2008, system of records notice. This SORN may be viewed at https://www.doi.gov/privacy/bia_notices. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records in NASIS are primarily retrieved by Name and a unique student identification code assigned by the system. Records may also be retrieved by any other keyword search such as gender, race, date of birth, SSN, grade, native language, tribe, attendance information, grades, discipline information, test and assessment histories, program enrollments, and health information; parent last and parent first name.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

The BIE staff and school administrators generate reports to meet day-to-day administrative and regulatory requirements primarily demographic data reports, which may include Name, Gender, NASIS ID Number, Birth Date, Student State ID, Staff Number, Staff State ID, Contact Information, Preferred Language, Race/Ethnicity Information, Federal Race/Ethnicity Designation, Hispanic/Latino Race/Ethnicity Determination, Date Entered US, Date Entered US School; Contact Information, Comments, and Emergency Contact Information.

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit Logs also collect information on system users such as username. System administrators and the information system owner have access to these activity reports.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data is collected from the student's parent or guardian during enrollment and is assumed to be accurate. School staff verify the accuracy of the information provided during enrollment with the parent or guardian providing the information. Several built-in data editors in NASIS validate information entered by a user.

Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

B. How will data be checked for completeness?

Data is collected from the student's parent or guardian during enrollment and is assumed to be complete. School staff check for completeness of the information at enrollment with the parent or guardian providing the information, ensuring all required information is provided.

Users are responsible for ensuring the completeness of the data associated with their user accounts. Data is checked for completeness during the account creation process.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

NASIS has the capability to crosscheck data to identify data discrepancies. The NASIS program staff reviews the reports on a regular basis and coordinate data updates with the designated school staff. NASIS has the Indian School Equalization Program Verification Report that is generated by the school administrator for student enrollment data quality check and makes the necessary updates.

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the currency of their records.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records are covered by Indian Affairs Records Schedule (IARS) Records Series 5400 – School Operations under multiple file codes and have been scheduled as permanent records by the National Archives and Records Administration (NARA) under Job No. N1-075-05-0001, approved on October 24, 2005. Records are maintained in the office of record for a maximum of 5 years. Records are cut-off at the end of the fiscal year. The records are then retired to the American Indian Records Repository which is a Federal Records Center. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the Department of the Interior (DOI) and NARA.

NASIS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

NASIS paper and electronic records have a permanent retention and are retired to the American Indian Records Repository (AIRR), which is a Federal Records Center. Subsequent legal transfer of the records to the National Archives of the United States will be jointly agreed to between DOI and NARA. Data disposition follows NARA guidelines and approved Records Schedule for transfer, pre-accession and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins, and the records management policies and procedures of the Bureau of Trust Funds Administration, Office of Trust Records, which is the office that provides records oversight and develops records retention and disposition schedules for the Bureau of Indian Affairs. System administrators dispose of DOI records by shredding or pulping for paper records, and degaussing or erasing for electronic records in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals due to the sensitive PII contained in NASIS. NASIS has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. NASIS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. Additionally, there are three tiers of Identification and Authorization present in NASIS, which further limits access to information. System and information access is based on the "least privilege" principle combined with a "need-to-know" in order to complete assigned duties. BIE manages NASIS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of NASIS user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Annually employees complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they have an understanding of their responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protecting against inappropriate use or disclosure to unauthorized individuals.

There is a risk that NASIS may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained in order to provide a

service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, based on the "least privilege" principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. NASIS has met BIE's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. Data is collected from the student's parent or guardian during enrollment and is assumed to be accurate. School staff verify the accuracy of the information provided during enrollment with the parent or guardian providing the information. Several built-in data editors in NASIS validate information entered by a user. NASIS has the capability to crosscheck data to identify data discrepancies. The NASIS program staff reviews the reports on a regular basis and coordinates data updates with the designated school staff. NASIS has the Indian School Equalization Program Verification Report that is generated by the school administrator for student enrollment data quality and makes the necessary updates.

There is a risk that information might be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. In regard to information handling and retention procedures, Office of Indian Education Programs is responsible for managing and disposing of BIE records in NASIS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued historical, cultural, and Tribal value. The Office of Indian Education Programs ensures only records needed to support its program, the Tribes, and Tribal members is maintained. Office of Indian Education Programs maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for

permanent safekeeping in accordance with retention schedules approved by NARA October 24, 2005, under Job Code N1-75-05-0005, Series 5400-School Operations. NASIS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off. Information collected and stored within NASIS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published BIA-22, Native American Student Information System (NASIS) system of records notice, 73 FR 40605, July 15, 2008, which may be viewed at: https://www.doi.gov/privacy/bia_notices. Additionally, a Privacy Act Statement (PAS) is on the Data Elements for Student Enrollment in Bureau-funded Schools form. The PIA, SORN, and PAS provide a detailed description of data elements and how an individual's PII is used.

There is a risk with the hosting of NASIS 2.0 at a non-DOI managed data center or that the vendor may not handle or store information appropriately according to DOI policy. NASIS 2.0 is hosted and administered within a DOI-approved data center. The data center is required to meet all Federal, National Institute of Standards and Technology (NIST), DOI and Indian Affairs, and NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, security control requirements. They must have an approved authority to operate (ATO) and are assessed as part of the information systems ATO being hosted in the data center. BIE manages system access using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of system user accounts.

In addition to the risk mitigation actions described above, the Bureau maintains an audit trail of activity sufficient to reconstruct security relevant events. The BIE follows the 'least privilege' security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of the system and data collected is relevant and necessary to the purpose for which NASIS was designed and supports the Indian Affairs mission. The system is used to administer BIE-funded schools by providing high quality data to authorized users. NASIS serves as the BIE's primary tracking and reporting system for students attending BIE-funded schools and for duty certifications of employees at such schools.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not Applicable. NASIS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Parents*

There are three tiers of Identification and Authorization present in the NASIS Application system; which are:

Administrative users (Tier 1). Contractor System Administrators, Database administrators, Network administrators, Application Developers, Help Desk / Support Staff and BIE/Bureau of Indian Affairs employees serving as System administrators. These users are required by DOI, Department of Homeland Security, Office of Management and Budget and National Institute of Standards and Technology (NIST) guidelines to be provided access the system using Homeland Security Presidential Directive-12 compliant screening process and DOI mandated personal identity verification (PIV) access cards. A PIV is a valid government-issued credential.

State/District Users (Tier 2). State Users are BIE employees who have PIV cards. These users have state level access to reports that use read-only data across all BIE-funded schools. There are two Tier 2 District Users at each school, one school administrator and one designee that because of their job function will have access to PII data. This level of access may also include BIE employees who have PIV cards. BIE employees with PIV cards are required to access the NASIS system using PIV authentication as prescribed for Tier 1 users. All others are required to use a NIST SP 800-63 compliant multifactor authentication mechanism to access the NASIS application.

Teachers, Parents, and Students (Tier 3). These NASIS users are also known as "portal users." They do not have access to PII data and following the assessment approach described in NIST SP 800-63 are not required to use multi-factor authentication. Users at this access tier are authorized to use simple username and password authentication. Teachers are only given access to data on a "least privilege" principle and "need-to-know" to perform official functions.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Users are only given access to data on a "least privilege" principle and "need-to-know" to perform official functions. BIE manages NASIS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of NASIS user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

Tier 1 and Tier 2 Account management – Users are only given access to data on a "least privilege" principle and "need-to-know" to perform official functions. Indian Affairs manages bureau users

and school's system administrator accounts using the automated IIS system. This includes establishing, activating, modifying, reviewing, disabling and removing of NASIS accounts. Accounts are established by the user initiating a request through IIS. Next, the IIS request is automatically sent to the supervisor for approval. After access is approved within IIS, the user completes the NASIS User ID/Password Request form, and has it signed by the Supervisor. The State User then sends the form and the Information Management and Technology (IMT) Awareness Training certificate, which includes Privacy Awareness Training, Records Management and Section 508 Compliance Training, and Controlled Unclassified Information (CUI) Training to the NASIS state edition system administrator to create the user account. The school level District User sends the same form and the IMT certificate to Infinite Campus to create the user account. Once an account has been created, the system administrator notifies the user via email of their user ID and temporary password with instructions that the user will be required to create a new password. Upon a change in a school NASIS system administrator (technical contact), the school contacts Infinite Campus by creating a Salesforce case to remove the technical contact and to create the new technical contact user account. Infinite Campuses support staff attach the NASIS designation form to the Salesforce case that is filled out by the district and must be signed off on by the school's principal or superintendent. Once the form is received back from the school with a current IMT certificate attached, a campus support staff creates the requested account.

Tier 3 Account Management – Teachers are only given access to data on a "least privilege" principle and "need-to-know" to perform official functions. For each school NASIS parent, student, and teacher; user accounts are managed by the schools NASIS System Administrator (Tier 2 District User). Each school is responsible for user account request, approval, provisioning, and review. The NASIS system administrator for the school uses the NASIS user module to manage accounts.

Infinite Campus Administrators have full but segregated administrative duties related to the onsite operation of NASIS. School System Administrators have view/edit access for students within assigned schools, manage user accounts, and act as the first level help desk administrators. Teachers have access to school level data based on authorized accesses and permissions. Principals are able to see information for students at their assigned school. BIE Senior Management are able to view and create reports for individual schools or districts and does not have access to information at the individual level.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The purpose of NASIS is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The NASIS system is not intended to monitor individuals; however the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring.

M. What controls will be used to prevent unauthorized monitoring?

NASIS has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring. NASIS System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. NASIS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users are required to consent to NASIS Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes

Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The NASIS audit trail includes system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- ☒ Security Guards
- ☐ Key Guards
- ☒ Locked File Cabinets
- ☒ Secured Facility
- ☒ Closed Circuit Television
- ☐ Cipher Locks
- ☒ Identification Badges
- ☐ Safes
- ☒ Combination Locks
- ☒ Locked Offices
- ☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- ☒ Password
- ☒ Firewall
- ☒ Encryption
- ☒ User Identification
- ☒ Biometrics (Applicable to NASIS 2.0)
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☒ Public Key Infrastructure (PKI) Certificates
- ☒ Personal Identity Verification (PIV) Card
- ☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- ☒ Periodic Security Audits
- ☒ Backups Secured Off-site
- ☒ Rules of Behavior
- ☒ Role-Based Training
- ☒ Regular Monitoring of Users' Security Practices

☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Associate Chief Information Officer is the Information System Owner. The Information System Owner, Information System Security Officer, and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in NASIS. The Information System Owner and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests access, redress, or amendment of records in consultation with the DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The NASIS Information System Owner and Information Systems Security Officer are responsible for the central oversight and management of the NASIS security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The NASIS Information System Owner, Information System Security Officer, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1- hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials.