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: education Learning Management System (eLMS)
Bureau/Office: Bureau of Indian Education (BIE)/Office of the Director
Date: August 4, 2022
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs 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 mission of the Bureau of Indian Education (BIE) is to provide students at BIE-funded schools with a culturally relevant, high-quality education that prepares students with the knowledge, skills, and behaviors needed to flourish in the opportunities of tomorrow, become healthy and successful individuals, and lead their communities and sovereign nations to a thriving future that preserves their unique cultural identities.

The education Learning Management System (eLMS) is a commercial-off-the-shelf, “contractor-owned, contractor-operated (COCO),” major application that provides the BIE a centralized system to support students, teachers, parent/guardians, administrators, Education Resource

Center (ERC) staff, and the Central Office staff. The eLMS is an online, cloud-based software program that provides a consistent platform for collaboration and aligning education standards and assessments with BIE selected curriculum and resources. The eLMS provides easy access to learning resources for individual students and/or groups, helping both teachers and parent/guardians with the educational goals of the students.

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), and Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99).

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other:

E. Is this information system registered in CSAM?

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

UII Code: 010-000002817, education Learning Management System (eLMS) System Security and Privacy Plan

☐ 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 pertaining to students, education staff, and parents or guardians may be in eLMS and are maintained under DOI system of records notice INTERIOR/BIA-22, Native American Student

Information System (NASIS), 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021). This SORN may be viewed at https://www.doi.gov/privacy/sorn.

□ No

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

□ Yes
☒ No

The eLMS does not require and OMB Control Number. However, information in eLMS is taken from NASIS, which is a centralized system that supports BIE schools. The following OMB Control Numbers apply to NASIS.

- OMB Control Number 1076-0122, Data Elements for Student Enrollment in Bureau-Funded Schools; Expiration Date: December 31, 2024
- OMB Control Number 1076-0134, Student Transportation Form: Expiration Date: May 31, 2025
- OMB Control Number 1076-0176, IDEIA Part B and C Child Count; Expiration Date: June 30, 2024

Section 2. Summary of System Data

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

☒ Name
☒ Education Information (K-12 Student Information, primarily Grades)
☒ Personal Email Address
☒ Other: Username, Password, names of education staff, parent/legal guardians; student name, NASIS student identification, and grades. Username and Password are collected for identification and authentication purposes and to manage user accounts. Personal email addresses are used to send notifications to parents and students.

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: Student grades which are recorded by education staff. All other information is obtained from NASIS using a secure/encrypted application programming interface (API).

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. Information will be shared between eLMS and NASIS by use of the OneRoster 1.2 (OR) API. The OR 1.2 standard addresses the exchange of student data (primarily about people, courses, enrollments, and grades) between different educational systems for the specific needs of K-12. The primary use-case is the exchange of data between a Student Information System (SIS) and a Learning Management System (LMS).

□ Other:

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

The intended use of the PII is to ensure appropriate access to the class content, assign teachers and students to classroom curriculum, document student's progress on the curricula, and allow parents/guardians to monitor their child's progress. The eLMS promotes distance learning and allows students, parents, and teachers direct access to educational content.

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

☒ Within the Bureau/Office: Information may be shared with BIE Federal employees and contractors acting in their official capacity in the performance of official functions. Data stored in eLMS is used to manage functionality. Only authorized users with a need-to-know are granted access to information. Users' access to information is controlled by their role (students, teacher, parent/guardian, administrator, or central BIE) and organization (classroom, school/district, ERC, or central BIE). For example, a teacher in one classroom cannot see information of students in a different teacher's classroom. Additionally, school administrators or BIE data analysts with authorization will have the ability to extract data for their organization for analytic and reporting purposes, particularly around student achievement and performance.

□ 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.*

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

☒ Contractor: Information may be shared with contractors providing information technology support services for routine maintenance, future system enhancements, technical and helpdesk support and as authorized pursuant to the routine uses contained in DOI system of records notice INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021). This SORN may be viewed at https://www.doi.gov/privacy/sorn.

□ Other Third-Party Sources:

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 can decline to provide information when parents/guardians complete the Student Enrollment Application for Students used with NASIS.

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

Except for student grades which are recorded by education staff, other information used with eLMS is not collected directly from an individual but is collected from NASIS using a secure/encrypted API.

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

☒ Privacy Act Statement: A Privacy Act Statement (PAS) is included on the Data Elements for Student Enrollment in Bureau-funded Schools form (OMB Control Number 1076-0122, Expires December 31, 2024) used with NASIS. The PAS provides detailed information on the authority and purpose of collecting PII, how PII is used and with whom the PII is shared, the applicable routine uses under the INTERIOR/BIA-22, and the voluntary nature of the collection, as well as impacts for not providing information. A PAS will also be posted on the eLMS site where individuals access the system.

☒ Privacy Notice: Privacy notice is provided through publication of this privacy impact assessment and the published DOI system of records notice INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021). This SORN may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.* A DOI security warning banner will be displayed to all users when accessing the system. The banner informs users that access is in accordance with agency policy for official use and limited personal use, that the system is subject to monitoring for lawful and security purposes, that all information including personal information is subject to monitoring, and users reminded that such monitoring occurs and there should be no expectation of privacy with respect to the use of eLMS. It also informs users that by logging into eLMS they acknowledge and consent to the monitoring of user actions, which includes evidence of eLMS User’s use, authorized or unauthorized, and may be used for civil, criminal, administrative, or other adverse action, and that unauthorized or illegal use may subject users to prosecution.

☐ None

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

Data is retrieved via the OR 1.2 API, which consists of school building information, User accounts including username or name (education staff, student, and parent/guardian), grading periods/terms, courses, sections and enrollments, and grading tasks.

I. Will reports be produced on individuals?

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

The primary report module from the platform is the course assessment reporting module. It provides detailed insights into individual and overall assessment items as well as student performance, which generally include names and grades. It provides quick insights into how individual students are performing on an assessment, including: Overall student performances, Average item performance, Categorization of High, Medium, and Low performing items, and Student performance for each item of the assessments. It also provides insights into the distribution of answers and analyzes metrics per item such as average score and points. Data is reported from applicable grade settings for assessments that have multiple choice or true/false answers and displays the scores that count in the final grade. Students, teachers, and administrators have access to the reports within the platform depending on their permission level. However, teachers are the primary users as reports measure overall student and student body performance.

Reports can also be generated from within the platform that track and monitor students' assessment progress, individually and collectively. For example, reports track the list of students who have taken the selected Managed Assessment (or curricula), the overall score each student received, the building (school) with which each student is affiliated, and the section in which the student is enrolled. The reports also contribute to the Gradebook functionality within the Platform, which, through the OR 1.2 API can be synced back to the NASIS for official report card reporting.

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 not collected from sources other than DOI records. NASIS is the source of the data used with eLMS, except for student grades which is recorded in eLMS by education staff. NASIS 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.

Parents, guardians, or legal caretakers can seek records about or on behalf of students that are maintained in this system of records and if the parent, guardian, or legal caretaker believes the records are not accurate can request corrections or the removal of material from the record by writing to the System Manager identified in the NASIS SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

B. How will data be checked for completeness?

NASIS is the source of the data used with eLMS, except for student grades which is recorded in eLMS by education staff. NASIS 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. Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts.

Parents, guardians, or legal caretakers can seek records on behalf of students that are maintained in this system of records and if the parent, guardian, or legal caretaker believes the records are not complete can request corrections or the removal of material from the record by writing to the System Manager identified in the NASIS SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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

NASIS is the source of the data used with eLMS, except for student grades which is recorded in eLMS by education staff. NASIS has the capability to crosscheck data to identify data discrepancies. The NASIS program staff review 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.

Parents, guardians, or legal caretakers can seek records on behalf of students that are maintained in this system of records and if the parent, guardian, or legal caretaker believes the records are not current can request corrections or the removal of material from the record by writing to the System Manager identified in the NASIS SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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 under the National Archives and Records Administration (NARA) Job No. N1-075-05-005, approved October 24, 2005. Records are cut-off at the end of the school year, maintained in the office of record for 5 years or when no longer needed for business purposes. The records are then retired to the American Indian Records Repository (AIRR) which is a Federal Records Center (FRC) for permanent safekeeping. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the United States Department of the Interior and NARA.

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three 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?

Data and information maintained within eLMS is retained under the appropriate NARA approved IARS. 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 Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of Indian Affairs' records retention schedule. 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 Departmental policy.

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 eLMS. The eLMS vendor leverages Amazon Web Services (AWS) data center facilities for the platform hosting infrastructure. The AWS data center regions utilized are FedRAMP compliant and have been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate impact level. While AWS maintains physical security and environmental safeguards of the hosting infrastructure, the vendor independently verifies its security posture and business continuity framework to internationally recognized standards for information security management system (ISMS) and has been accredited with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013 certification as well as American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC) 2 compliance for Service Organizations. The vendor controls associated with the ISO/IEC 27001:2013 certification, and AICPA SOC 2 compliance are based on NIST standards and are audited annually by an independent assessment organization during the renewal process. The vendor uses an external vendor security management platform based on industry standard frameworks, and includes supporting documentation, audits, and certifications to provide customers with access to their security profile, which includes annual security documents, attestations, and certifications regarding eLMS's ongoing security posture. Access to this security profile is available to customers upon request and available throughout the life of the agreement. The eLMS vendor has gone to great lengths to secure the data collected and stored within the eLMS. The vendor has implemented physical, technical, and administrative security controls to ensure the security of the data and limited access only to authorized users.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients or for unauthorized purposes. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access is based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. 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 awareness 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 understand 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, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that eLMS 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. The eLMS gathers and holds very few PII related data elements. However, when it does gather this information, it is directly related to the information required for the functioning of eLMS, no extraneous data is collected. 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 of the information 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. eLMS meets BIE's information system security requirements, including operational and risk management policies.

There is a risk of maintaining inaccurate information. This risk is mitigated as the data being brought into the eLMS is verified by School/District and BIE Staff for accuracy, currency, and completeness. Additionally, data is periodically checked to ensure changes to the source system (NASIS) are updated in eLMS. Students, parents, and teachers have appropriate access to view their records and if an individual believes their information in inaccurate after collection, may submit a request correction or the removal of material from records within the system that is deemed to be inaccurate, as described by 43 CFR Part 2, Subpart K. These requests are submitted in writing to the System Manager identified in the INTERIOR/BIA-22 SORN.

There may be a risk associated with the collection of information from other DOI systems. All data transfers use validated APIs over secure links with data encrypted as it is transferred. This applies to data being extracted from NASIS into the eLMS and from the eLMS into NASIS.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The BIE is responsible for managing and disposing of BIE records in eLMS as the information owner. BIE ensures only records needed to support its program, Tribes, and Tribal members is maintained. Records are maintained under records series 5400 – School Operations approved by NARA under Job Code N1-075-05-0005. Records are cutoff at the end of the school year, maintained on the office of record for 5 years or when no longer needed for current business operations, at which time they are transferred to the AIRR, a FRC for permanent safekeeping. Records in this system have a permanent retention schedule due to their continued historic value to Tribes. eLMS system usage records are covered by the DRS 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. Information collected and stored within eLMS 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 DOI system of records notice INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021), viewed at https://www.doi.gov/privacy/sorn. Additionally, a PAS is included on the Data Elements for Student Enrollment in Bureau-funded Schools (OMB Control Number 1076-0122) form used with NASIS and will be posted on the eLMS system entry screen. The PIA, SORN, and PAS provide a detailed description of system source data elements and how PII is used. As the records in eLMS are collected from NASIS, individuals may submit Privacy Act requests for access or amendment of records to the System Manager identified in the INTERIOR/BIA-22 NASIS SORN.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy.

eLMS is hosted and administered within a DOI-approved and FedRAMP-certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP certification. The data residing in the system is backed up on a nightly basis.

In addition to the risk mitigation actions described above, the BIE maintains an audit trail of activity sufficiently enough 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. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, Controlled Unclassified Information, Paperwork Reduction Act, and Section 508 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: The use of the system and data collected is relevant and necessary to the purpose for which eLMS was designed and supports the BIE mission of providing students at BIE-funded schools with a culturally relevant, high-quality education that prepares students with the knowledge, skills, and behaviors needed to flourish in the opportunities of tomorrow, become healthy and successful individuals, and lead their communities and sovereign nations to a thriving future that preserves their unique cultural identities.

☐ 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. The eLMS 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/Guardians

Users of the eLMS consist of students, teachers, and parents/guardians.

Students: Students access eLMS using a Username and Password. The Username and Password are provided by local IT Staff or Teacher when a computer is issued to the student. Both the Username and Password are provided to the student by their school. Students are only allowed to view their own PII.

Parents/Guardians: Parents/Guardians access eLMS using a Username and Password. Initially the school provides the parents with an access code that allows the parent to register with the eLMS. Parents have access to their own PII and the PII of their children.

Teachers: Teachers access eLMS using a Username and Password. The Username and Password is created during the initial login to eLMS. Teachers have access to their own PII as well as that of the students assigned to their class.

Vendor (Contractors and Developers), and School System Administrators access eLMS using a Username and Password.

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

User access to data is based on the “least privilege” principle and “need-to-know” to perform official functions. BIE manages user accounts using the IIS, a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of 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.

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

☒ No

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

☒ Yes. *Explanation*

The purpose of eLMS 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 eLMS 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 to prevent unauthorized monitoring.

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

eLMS can audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system to prevent unauthorized monitoring. eLMS 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. eLMS 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 BIE users will be required to consent to DOI Rules of Behavior. BIE users must complete annual IMT Awareness Training before being granted access to the DOI network or any DOI system, and annually thereafter. Students and Parents/Guardians are provided rules of behavior in the Student Handbook.

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 eLMS audit trail will include 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.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☐ Personal Identity Verification (PIV) Card
☒ Other. Username and password

(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.

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 BIE Deputy Associate Chief Information Officer is the Information System Owner. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in eLMS. The ISO and the Privacy Act System Managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the IA Associate Privacy Officer.

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 eLMS ISO and ISSO are responsible for the central oversight and management of the eLMS 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 eLMS ISO, ISSO, 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 one 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 IA Associate Privacy Officer. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act, the Family Educational Rights and Privacy Act (FERPA) and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.