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: "Box" Enterprise Cloud Content Collaboration Platform Implementation
Bureau/Office: Bureau of Indian Education, Division of Education Technology Programs Operations
Date: August 25, 2023
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?

A Privacy Threshold Analysis (PTA) was performed February 14, 2023, indicating that a Privacy Impact Assessment (PIA) must be completed. This PIA is being completed to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559), the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101), and Privacy Act of 1974.

The Bureau of Indian Education (BIE) is implementing the Box Enterprise Cloud Content Collaboration Platform, a FedRAMP certified software-as-a-service solution. This platform provides a secure way to share files and improve collaboration with external users. In addition to

file sharing, Box provides an enterprise content platform and safe workspace for internal and external teams to collaborate in a central workspace to create, edit, review, and share files and folders.

The primary use of Box is to collect and collaborate on school assessment data from Bureau Funded and Tribally Controlled Schools which will be compared and compiled with BIE Unified Assessment Data, provided to BIE in aggregate for statutorily required public reporting to comply with the Every Student Succeeds Act (ESSA).

Box will also be used to create a Digital Asset Management (DAM) library system for the media being developed and collected for BIE's Strategic Transformation and Education Plan initiative.

The Box uses Active Directory (AD) authentication. AD authentication for User access is covered under the Department of the Interior (DOI) Enterprise Hosted Infrastructure (EHI) PIA. For additional information on User authentication please see the EHI PIA on the DOI Privacy website: https://www.doi.gov/privacy/pia.

C. What is the legal authority?

- Every Student Succeeds Act (ESSA) (Pub. L. 114-95)
- Elementary and Secondary Education Act of 1965 (Pub. L. 89-10)
- Adequately Yearly Progress (25 CFR Part 30)

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: *Describe*

E. Is this information system registered in CSAM?

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

☒ No

Box is not registered in CSAM because it is being replaced by XACTA 360. The XACTA 360 tracking number for Box is BIA-0030-GSS.

UII Code: 010-000002656, Box System Security and Privacy Plan (SSP)

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 Box pertaining to individuals who require access to Departmental networks, information systems, and e-mail services are maintained under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)**,** 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021).

☒ No

Box is not a Privacy Act system of record as defined at 5 U.S.C. 552a (5). The system does not collect personally identifiable information (PII) directly from individuals. Box is a tool which will temporarily store data and files for internal and external collaboration. Files uploaded to Box may include data about teachers and students which are maintained under DOI system of records notice INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605, (July 15, 2008), modification publish at 86 FR 50157 (September 7, 2021), which may be viewed at https://www.doi.gov/privacy/sorn.

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

☐ Yes: *Describe*

☒ No

There are no forms associated with Box. Box does not actively nor directly collect PII from individuals and does not maintain the contents of the files submitted through Box. The information collections listed below are for transparency as they may be the source of the information included in the reports submitted using Box.

The BIE serves as the State Education Agency (SEA) for BIE-funded schools, which means it must ensure schools comply with U.S. Department of Education statutory and regulatory requirements. The assessment and accountability requirements under ESSA, and under 25 CFR 30.105 and 25 CFR 30.111, are submitted to the U.S. Department of Education as a part of their ED*Facts* information collection (OMB Control Number 1850-0925, ED*Facts* Data Collection School Years 2022-23, 2023-24, and 2024-25 (With 2021-22 Continuation), Expires June 30, 2025) and Consolidated State Performance Report (Part I and Part II) (OMB Control Number 1810-0614, Expires July 31, 2015). Some data may be obtained from the BIE Standards, Assessments, and Accountability System Waiver (OMB Control Number 1076-0191, Expires 07/31/2023) documentation.

Data Elements for Student Enrollment in Bureau-funded Schools (OMB Control Number 1076-0122, Expires 12/31/2024)

Section 2. Summary of System Data

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

☒ Name (Teacher and Student)
☒ Gender
☒ Birth Date (Student)
☒ Group Affiliation
☒ Disability Information
☒ Education Information
☒ Race/Ethnicity
☒ Tribal or Other ID Number
☒ Other: Box does not collect PII directly from individuals. However, Box may contain documents uploaded for temporary storage and collaboration that may include a wide range of PII. Any PII contained in these documents is extracted from other original records, which may include Teacher ID, Student Information, including: State Student ID Number (Mississippi Student Information System Number: A unique number or alphanumeric code assigned to a student by a school, school system, a state, or other agency or entity), DRC Student ID (A unique number assigned to a unique MSIS ID/District Code for an admin), Grade, Gender, Ethnicity, Disability, Individualized Education Plan, Section 504, Limited English Proficient Status, Retester (Used to indicated whether a student is a first-time tester or retesting and used to determine how the student is identified in reports).

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: *Describe*

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 *Describe*
☒ Other: The system does not collect PII directly from individuals. Box is used to collect data needed for reports via the Box Secure File Transport Protocol. Data, in the form of reports, is submitted in various file formats: .doc, .pdf, .xml, .cvs.

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

The system does not collect PII directly from individuals. Box is used as a secure file transport tool. The PII is used only for associating data elements to an individual to ensure accurate analysis of data for reporting. The data is de-identified before aggregate reports are produced and reported to the U.S. Department of Education to comply with the ESSA.

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 employees acting in their official capacity and in the performance of official functions related to collecting and reporting data to the U.S. Department of Education to comply with ESSA reporting requirements.

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

Information may be shared with 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 INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605, (July 15, 2008), modification publish at 86 FR 50157 (September 7, 2021), and INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021).

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

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.*

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

Information is not collected directly from individuals but obtained from school enrollment, grades, attendance, and other school records associated with the Native American Student Information System and are covered under the NASIS SORN.

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.*

Box does not actively nor directly collect PII from individuals, does not maintain the contents of the files submitted using Box, and is not a system of records. The Privacy Act statement described below is for transparency as the information collection may be the source of the information included in the reports submitted using Box.

A Privacy Act Statement is included on the Data Elements for Student Enrollment in Bureau-funded Schools form (OMB Control Number 1076-0122, Expires 12/31/2024).

This information is collected as provided by 5 U.S.C. 552a. The Office of Indian Education Programs is authorized to collect this information in accordance with Public Law 95-561; 98-511;99-89; and 100-297. The information will be used to determine the level of funding to be distributed by formula to BIE funded elementary and secondary schools. Weighted student units, the value of basic and specialized instructional and residential programs, are used to calculate the distribution of funds. The information may be disclosed to appropriate Department of the Interior and Congressional Offices for policy and budgetary purposes.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment, the published INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605, (July 15, 2008), modification publish at 86 FR 50157 (September 7, 2021), the individuals may view the NASIS PIA for information on how BIE manages student data, and INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021). These SORNs may be viewed at http://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

At logon to the network, 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 Box are not retrieved by name or unique identifier, but by a generic file name assigned to student performance data reports.

I. Will reports be produced on individuals?

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

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

Reports are not produced on individuals. Annual student performance data in reports includes metrics and do not identify specific students.

Section 3. Attributes of System Data

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

School administrators who submit performance reports or metrics are responsible for its accuracy.

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.

Parents and legal guardians can seek records about themselves and their children that are maintained in the NASIS system of records and if the individual 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 or by contacting the Indian Affairs (IA) Associate Privacy Officer (APO). Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

B. How will data be checked for completeness?

School administrators who submit performance reports or metrics are responsible for its completeness.

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.

Parents and legal guardians can seek records about themselves and their children that are maintained in the NASIS system of records and if the individual 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 or by contacting the IA APO. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

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

School administrators who submit performance reports or metrics are responsible for ensuring it is current.

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

Parents and legal guardians can seek records about themselves and their children that are maintained in the NASIS system of records and if the individual 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 or by contacting the IA APO. Access

procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

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 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 and the end of the fiscal year, maintained in the office of record for five years, and 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 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 Box are retained under the appropriate NARA approved Indian Affairs Records Schedules (IARS). Data dispositions follow 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 Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of IA's 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 Box. Box 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. Box is rated as a FISMA moderate system and requires

management, operational, and technical controls established by NIST Special Publication 800-53, Security and Privacy Controls for 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. System and information access is based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIE manages Box 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 Box 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 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 Box 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 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. Box meets BIE's information system security requirements, including operational and risk management policies.

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 Box as the information owner. The BIE ensures only records needed to support its program, Tribes, and Tribal members is maintained. BIE 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 under Job Code N1-075-05-005: Records series 5400 – School Operations, approved October 24, 2006. Box 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 Box 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 INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605, (July 15, 2008), modification publish at 86 FR 50157 (September 7, 2021), which may be viewed at https://www.doi.gov/privacy/sorn, and associated NASIS PIA. Additionally, a Privacy Act Statement (PAS) is provided in the Data Elements for student Enrollment in Bureau-funded Schools form (OMB Control Number 1076-0122). The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

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. Box 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. 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 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 multifactor 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 SP 800-53. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information (CUI) 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 are relevant and necessary to the purpose for which Box was procured supports the Indian Affairs mission as the State Education Agency (SEA) for BIE-funded schools, which means it must ensure that those schools comply with U.S. Department of Education statutory and regulatory requirements under ESSA, and under 25 CFR 30.105 and 25 CFR 30.111.

☐ 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. Box 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: *Describe*

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 Box user accounts using the Identity Information System, a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of Box 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.

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 privacy terms and conditions and the following 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 Box 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 Box 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, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

Box can audit the usage activity within the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring. 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. System Administrators assign User roles based on the principle of 'least privilege' and perform due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to Box Rules of Behavior. Users must complete annual IMT Awareness Training, which includes Privacy Awareness Training, Records Management

and Section 508 Compliance training, and 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 Box 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. *Describe*

(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. *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 BIE Deputy Associate Chief Information Officer serves as the Information System Owner (ISO) for Box. The ISO, Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for oversight and management of security and privacy controls and the protection of Indian Affairs information processed and stored by Box. The ISO is responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by Indian Affairs. The ISO is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, 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 BIE ISO and ISSO are responsible for daily operational oversight and management of the system's 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 ISO, the ISSO, and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the IA Associate Privacy Officer.