U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Box Enterprise Cloud Content Collaboration Platform)
System or Project Acronym:	BOX
Date submitted for review:	May 20, 2026
System Operational Status:	Operational

Point of Contact

Name:	Adrienne Brooks-Hill
Title:	Privacy Officer
Office:	Office of the Chief Information Officer
Phone:	202-208-1605
E-mail:	DOI_Privacy@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☐ Significant Modification
☒ Other: Describe below

Existing Information System under Periodic Review.

2. What is the purpose of the system or project?

Box.com is a FedRAMP-authorized Software-as-a-Service (SaaS) platform used by DOI Interior Business Center (IBC) and authorized customer users to securely transfer, receive, store temporarily, and collaborate on files in support of official business. The primary purpose of Box is secure file transfer and controlled content sharing, including the ability to exchange files with authorized internal and external users when email or other transfer methods are not appropriate for sensitive or large files.

Box is not intended to serve as the authoritative system of record for the business records transferred through

the platform. The records stored or transferred through Box remain governed by the originating program, system of record, applicable SORN, applicable records schedule, and the business process for which the records were created or received.

Box directly maintains platform information necessary to support account access, authentication, authorization, audit logging, file transfer, collaboration, security monitoring, and system administration. This may include user account information, email address, user ID, login events, IP address, file access events, sharing activity, timestamps, and related system metadata.

Box may contain files with PII when authorized users upload or transfer official records that include PII. The PII in those files is not originally collected by Box for independent Box purposes; it is uploaded by authorized users to support secure file transfer and collaboration. Access to files is limited through role-based permissions, folder-level access, sharing controls, authentication requirements, audit logging, and other security safeguards.

Box is not intended to be used to retrieve records by personal identifier as a primary business function. However, because authorized users may search file names, document titles, metadata, or content that may include a person's name or other identifier, Box may technically permit retrieval of files containing PII. This incidental search capability does not make Box the authoritative system of records for the underlying content. The applicable SORN and records schedule are determined by the originating record type and business owner.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

UII Code -010-000002434, Box Enterprise Cloud Content Collaboration Platform

4. What legal authorities authorize the collection and use of data in this system or project?

- 5 U.S.C. 5101, et seq., Government Organization and Employees;
- 31 U.S.C. 3512, et seq., Executive Agency Accounting and Other Financial Management Reports and Plans;
- 31 U.S.C. 1101, et seq., the Budget and Fiscal, Budget, and Program Information;
- 5 CFR part 293, subpart B, Personnel Records Subject to the Privacy Act; 5 CFR part 297, Privacy Procedures for Personnel Records;
- Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers;
- Public Law 101-576 (Nov. 15, 1990), the Chief Financial Officers (CFO) Act of 1990;
- E-Government Act of 2002;
- Federal Information Security Modernization Act of 2014; and
- OMB Circular A-130.

These authorities support DOI's use of secure information technology services to manage, protect, transfer, and collaborate on official records and information in support of authorized acquisition, financial management, human resources, legal, administrative, and other official business functions. The legal authority for the underlying records transferred through Box remains with the originating program, system, or business process.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

Box may contain records that include PII when authorized users upload, transfer, receive, or collaborate on official files. Box is not the authoritative system of record for the underlying file content. The underlying records remain governed by the originating system, program office, customer agency, applicable SORN, and applicable NARA-approved records schedule.

Box is used primarily as a secure file transfer and controlled collaboration platform. It is not intended to maintain a group of records about individuals for retrieval by personal identifier as a primary system purpose. However, because authorized users may search or filter file names, document titles, metadata, user activity, or file content that may include personal identifiers, the applicability of a SORN is determined by the type of records stored or transferred and the originating business process.

Records in the Box Enterprise Cloud Content Collaboration Platform application are maintained under the Office of Personnel Management (OPM) government-wide system of records notices (SORNs) and those for DOI:

- OPM/GOVT-1, General Personnel Records, December 11, 2012 (77 FR 73694); modifications published February 2, 2022 (87 FR 5874) and August 17, 2023 (88 FR 5658);
- OPM/GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records, June 19, 2006 (71 FR 35356); modification published February 2, 2022 (87 FR 5874), and the
- DOI SORN, DOI-85 Payroll, Attendance, Retirement, and Leave Records, July 19, 2018 (83 FR 34156).

These SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

Box does not retrieve records by personal identifier beyond user account metadata; therefore, Box is not the system of record. Records stored in Box belong to originating systems.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last) ☒ Home telephone number ☒ Employment or resume info

☒ Aliases/nickname
☒ Driver's license
☒ Citizenship
☒ Legal Status
☒ Sex
☒ Race or ethnicity
☒ Date of birth
☒ Place of birth
☒ Personal cell phone number
☒ Tribal or other ID number
☒ Military records
☒ Personal Email
☒ Mailing or home address
☒ Religious preference
☒ Mother's maiden name
☒ Marital status
☒ Spouse Information
☒ Child or family information
☒ Emergency contact info
☒ Financial information
☒ Education information
☒ Other: Describe below
☒ Full or Truncated SSN
☐ Physical characteristics
☐ Biometrics or facial recognition
☐ Vehicle information
☐ Passport information
☐ Travel information
☐ Parent's name
☒ Credit card number
☐ Nationality
☒ Disability Information

The PII listed above reflects what documents stored in Box contain and not Box itself. Box collects information on user access and logins, including internet protocol (IP) addresses, login times and dates, user identification (IDs), group affiliation, security clearance, medical information, and specific event types. Box directly collects only user credentials (username, authentication logs, IP addresses, login times, event metadata). Files uploaded into Box may contain PII as part of existing records from other systems of record, which are covered under their own authorities and SORNs (e.g., OPM/GOVT-1, DOI-85). Box itself is not the system of record for those files .

2. What is the source for the PII collected? Check all that apply.

☒ Individual
☒ Federal Agency
☒ Tribal Agency
☒ Local Agency
☒ DOI Records
☐ Third Party Records
☐ State Agency
☐ Other: *Describe Below*

3. How will the information be collected? Check all that apply.

☐ Paper Format
☐ Email
☐ Face-to-Fact Contact
☒ Website
☐ Fax
☐ Telephone Interview
☐ Shared Between Systems: *Describe*
☐ Other: *Describe*

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

Box uses user account and access metadata to authenticate users, enforce permissions, support secure file transfer, maintain audit logs, monitor system activity, support incident response, and administer the platform.

PII contained in uploaded or transferred files is used by authorized users only for the official business purpose associated with the originating record or transaction. Box does not independently use the content of transferred files to make determinations about individuals. Box is used to securely transfer, receive, temporarily store, and collaborate on files; the underlying records remain controlled by the originating program or system owner.

5. How does this project limit the collection and use of PII to only what is necessary?

Box directly collects only the minimum platform information required for authentication, authorization, access

control, audit logging, secure file transfer, collaboration, and system administration. This includes limited user account and system metadata such as username, email address, user ID, login timestamp, IP address, sharing activity, and file access events.

PII contained in uploaded files is limited by the originating business process. Users are responsible for uploading only information necessary for official business and for applying appropriate sharing restrictions. Access controls, permissions, folder restrictions, link-sharing controls, audit logging, retention controls, and user training reduce unnecessary collection, use, disclosure, and retention of PII in Box.

Section 3: Data Sharing and Individual Rights

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

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☐ **Other Third-Party Sources:** Describe how the data will be used below.

Within the Bureau/Office: PII will be shared within the DOI Interior Business Center (IBC) to support administrative functions such as human resources (HR), financial management, and contract administration. Only authorized personnel with a need-to-know basis will have access.

Other Bureaus/Offices: PII may be shared with other DOI bureaus and offices as required for payroll, personnel records management, acquisition services, and financial transactions. The sharing is limited to specific personnel within DOI with appropriate security and privacy safeguards in place.

Contractor: Box, Inc. contractors may assist with system maintenance and technical support under security agreements.

Other Federal Agencies: If necessary, information may be shared with federal agencies such as the Office of Personnel Management (OPM) for HR-related functions, Treasury Department for financial transactions, or other federal entities under specific agreements. Information shared with other federal agencies is as permitted under the routine uses identified in OPM/GOVT-1, OPM/GOVT-7, and DOI-85, which may be viewed at https://www.doi.gov/privacy/sorn.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

No formal Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Interconnection Security Agreement (ISA) is required for Box as used by IBC, because Box does not independently disseminate records to external agencies. Information shared outside DOI occurs through the originating systems of record

under their established authorities and routine uses (e.g., OPM/GOVT-1, OPM/GOVT-7, DOI-85). If any customer agency establishes an integration requiring a formal agreement, such agreements will be executed by that system owner and cited in their respective documentation.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☐ 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*.

The PII found in Box is uploaded from the originating system that provides individuals the right to deny or consent under the Privacy Act of 1974. Individuals cannot consent or decline directly within Box. However, individuals are required to provide PII when it is necessary for employment, payroll processing, security clearance, or federal record-keeping to fulfill DOI Interior Business Center operations.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☒ Privacy Act Statement:
☒ Privacy Notice:
☐ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

Privacy Act Statement: At the point of collection from the originating system, that system provides a Privacy Act Statement. Box merely uploads PII from the originating system.

Privacy Notice: Box provides a detailed webpage notice for all users that discusses the uses, collection, sharing and disclosure of information as well as protection of PII. The Box Privacy Notice may be viewed at https://www.box.com/legal/privacypolicy.

Upon login a U.S. Government Warning and Consent banner appears. The banner notifies users that Box is for authorized use only and of system monitoring. Additionally, publication of this privacy impact assessment will serve as notice along with its associated SORNs, INTERIOR/DOI-85, Payroll, Attendance, Retirement and Leave Records; OPM/GOVT-1, General Personnel Records and OPM/GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records. The SORNs associated with this system may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

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

Box is not intended to be used as a system for retrieving records about individuals by personal identifier. The primary retrieval methods are folder location, document title, file name, project or transaction context, metadata, date, owner, sharing status, and other collaboration or file-management attributes.

However, authorized users may be able to search for names, email addresses, or other personal identifiers if those identifiers appear in file names, document titles, metadata, audit logs, or file content. This capability is incidental to secure file transfer and collaboration and does not make Box the authoritative system of record for

the underlying content. The applicable SORN is determined by the originating record type and business process. Box platform metadata and audit records may be retrieved by user ID, username, email address, IP address, or other access-related identifiers for security, audit, incident response, and system administration purposes.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

Box does not produce substantive program reports on individuals or make determinations about individuals. However, Box may produce administrative, security, audit, access, and activity reports that identify individual users. These reports may include username, user ID, email address, login attempts, file access events, sharing activity, IP address, timestamps, and configuration or permission changes.

These reports are used for security monitoring, access review, incident response, compliance, and system administration. Access to these reports is restricted to authorized system administrators, security personnel, and other personnel with an official need to know.

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

Box data collected from sources, such as other federal and state agencies, will be verified for accuracy through automated validation processes and manual review by authorized personnel. When possible, data will be checked against official records, government-wide databases, and internal DOI records to ensure consistency and correctness. Additionally, data integrity checks will be performed periodically to detect and correct discrepancies.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Box is used primarily as a secure file transfer and controlled collaboration platform. Retention and disposition of files in Box depend on the recordkeeping status and business context of the content. The authoritative record copy remains governed by the originating program, system of record, applicable SORN, and applicable NARA-approved records schedule.

Where Box contains temporary working copies, transfer copies, duplicate copies, convenience copies, or collaboration copies, those materials should be deleted when no longer needed for the business purpose for which they were uploaded or transferred, unless subject to litigation hold, audit, investigation, FOIA, Privacy Act request, records freeze, or other preservation requirement.

Where a program uses Box to maintain official record copies, the program must identify and apply the applicable records schedule and coordinate with the Records Officer. Box content must not be treated categorically as non-record or transitory if it is being used as the official recordkeeping location.

Box platform audit logs, account metadata, access events, and security records are retained in accordance with

applicable DOI cybersecurity, audit, system maintenance, FedRAMP, and records management requirements.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

Box data collected from sources, such as other federal and state agencies, will be verified for accuracy through automated validation processes and manual review by authorized personnel. When possible, data will be checked against official records, government-wide databases, and internal DOI records to ensure consistency and correctness. Additionally, data integrity checks will be performed periodically to detect and correct discrepancies.

The Box uses scheduled data reviews, automated updates, and user notifications to maintain up-to-date information. Regular audits are conducted by Box, Inc. to verify the timeliness of data, and records that have not been updated within a defined period may trigger a review process. Data updates from authoritative external sources (e.g., financial systems) are synchronized through secure Application Programming Interface integrations or data refresh cycles.

To ensure data completeness, the Box Enterprise Cloud Content Collaboration Platform enforces mandatory input fields, validation rules, and structured data entry processes. DOI IBC system administrators will perform periodic audits to identify missing or incomplete records. Automated validation checks by Box will flag incomplete submissions, prompting users to enter the necessary information before the data is accepted into the system.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

Box logs detail types of events such as login attempts, configuration changes, file access, and use of system utilities. All events are time-stamped with their date and time to provide a temporal context. Information about the terminal identity or location is logged to establish where events occur within the system. Box captures the source of events, including user IDs and network addresses, to identify the origin. Monitoring is strictly for system security and access to logs is restricted.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

Risks are mitigated by the controls implemented to safeguard PII and secure the network in accordance with the overall moderate security categorization pursuant to the Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. A moderate security categorization indicates that the potential impact of a security breach could result in serious adverse effects on organizational operations, assets, or individuals. Below are the risks and mitigations for each stage of the informational lifecycle DOI IBC implements to safeguard the data.

Collection Risk – Box Enterprise Cloud Content Collaboration Platform bears the potential risk of data inaccuracies and of uploading data that does not pertain to Box. To mitigate these risks, Box follows a multi-layered validation process with automated checks against existing DOI IBC records to ensure consistency, and periodic audits that Box system administrators perform to identify and correct discrepancies.

Use Risk – Unauthorized access, data breaches, and improper disclosure of PII are potential privacy risks. The IBC Information System Owner mitigates these risks by implementing access controls to limit data entry to authorized personnel; restricting data access on a need-to-know basis using role-based access controls (RBAC), employing monitoring tools, and security reviews to detect improper use. Security control implementations include multi-factor authentication (MFA) for user access, encryption of data at rest (DAR) and in data in transit (DIT), and access control policies to prevent unauthorized data usage.

Box, Inc., which maintains a FedRAMP authorization for its cloud service product, is responsible for all audits of its platform. Box uploads its vulnerability scans to a continuous monitoring file for the agency, enabling the DOI Information System Security Officer (ISSO) to verify these vulnerability scans.

For an example of access control, general users access only their assigned department files. Managers access team-level documents. Box system administrators maintain Box platform security, but do not have direct access to user files. Also, access to logs is restricted to protect against metadata/log data use beyond security monitoring.

Processing Risk – To mitigate improper sharing of PII or accidental disclosure, the ISSO enforces data sharing agreements and data encryption in transit and at rest. The system's design and security measures, including MFA, protect data during processing, limiting unauthorized access and potential misuse. External sharing is prohibited unless required by a routine use listed in the applicable SORN. All contractors sign agreements requiring compliance with DOI privacy policy.

Retention and Disposal Risk - Retaining data past its operational use could increase the risk of unauthorized access. Adherence to DOI data destruction policies ensures secure and timely deletion of data when it is no longer needed, reducing the risk of unauthorized access or misuse.

These mitigations collectively reduce the system’s privacy risk profile and support DOI’s obligation to protect individual information and promote accountability.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

The Box Enterprise Cloud Content Collaboration Platform primarily stores, organizes, and facilitates secure access to existing records. It does not generate new insights or predictive patterns through data aggregation.

3. Will the new data be placed in the individual’s record?

☐ Yes: *Provide explanation below*
☒ No

Box does not generate new substantive data or inferences about individuals through aggregation or analytics as part of the approved secure file transfer use case. Box stores, transfers, and supports controlled collaboration on existing files uploaded by authorized users.

Box may generate platform metadata, audit logs, file access events, sharing activity, timestamps, and other administrative records related to user activity. These records are used for security monitoring, access control, incident response, compliance, and system administration, not to make program determinations about individuals.

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

☐ Yes: *Provide explanation below*
☒ No

The Box Enterprise Cloud Content Collaboration Platform does not perform automated decision-making, or analysis affecting individuals. It only facilitates document storage and retrieval.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

N/A. New data is not derived or created. The Box follows a multi-layered validation process, including user verification at data entry to prevent errors, automated checks against existing DOI IBC records to ensure consistency, and periodic audits by Box system administrators to identify and correct discrepancies for *existing* data.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☒ Yes
☐ No, *Proceed to Section 7.*

Box.com includes embedded AI-enabled capabilities within the commercial SaaS platform, including capabilities that may support enhanced search, metadata extraction, document summarization, information extraction, and AI-assisted content generation. DOI's approved use of Box in this PIA is limited to secure file transfer, controlled file sharing, temporary storage, and collaboration in support of official business.
Box is not used to make automated decisions about individuals, determine eligibility, score or rank individuals, generate employment or benefits determinations, or replace human review. Any AI-enabled functionality available within the platform may only be used as an assistive feature to help authorized users locate, understand, summarize, or manage content already stored or transferred within Box. AI outputs may not be used as the sole basis for any official decision or action affecting an individual.
PII may be present in files uploaded to or transferred through Box. To the extent AI-enabled features interact with files, prompts, metadata, or outputs that contain PII, the use remains subject to DOI privacy requirements, source-system SORN coverage, records management requirements, access controls, audit logging, and human review. Box does not serve as the authoritative system of record for the underlying content transferred through

the platform; the originating system, program, or business owner remains responsible for the underlying records and applicable SORN coverage.

2. How are models validated for fairness, accuracy, and transparency?

Box AI capabilities are vendor-managed as part of the Box.com SaaS environment. DOI does not train, fine-tune, or independently modify the underlying AI models. DOI relies on vendor-provided documentation, FedRAMP security review materials, contractual requirements, and DOI security/privacy review processes to understand model behavior, limitations, data handling, and safeguards.

For DOI use, AI outputs are treated as assistive and advisory only. Authorized users are responsible for reviewing, validating, and correcting any AI-generated summary, extracted information, metadata, or content before relying on it for official business. AI outputs may not be used as the sole basis for decisions or actions affecting individuals.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☒ No

Box does not make AI-based decisions that affect individuals. The approved DOI use of Box is secure file transfer, controlled file sharing, temporary storage, and collaboration. AI-enabled features, where available, are assistive only and do not determine rights, benefits, employment, eligibility, access to services, legal status, or other consequential outcomes. Any official decision involving records transferred through Box is made by authorized personnel under the originating business process, not by Box AI.

4. Are safeguards in place to prevent bias or unintended consequences?

☒ Yes
☐ No

Safeguards include human review of AI-assisted outputs, role-based access controls, tenant and folder permissions, audit logging, user training, FedRAMP security controls, and limits on using Box AI outputs for official decisions. Box AI is not approved to independently classify, score, rank, recommend, or make determinations about individuals. Users remain responsible for validating any AI-assisted summary, metadata extraction, or content generation before use.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☒ Yes
☐ No

The AI models are maintained by Box as part of the vendor-managed SaaS platform. DOI does not provide training data, retrain models, or modify model parameters. DOI relies on vendor lifecycle management, security documentation, contractual controls, FedRAMP-related review, and DOI oversight processes to monitor changes that may affect privacy, security, or operational use. Material changes to AI functionality, data use, model

behavior, or approved DOI use would require additional privacy review.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☒ No

DOI does not use federated learning with Box. DOI does not train Box AI models using DOI content, user prompts, metadata, or files transferred through Box. AI-enabled features operate, where available, as vendor-provided assistive capabilities within the Box SaaS environment and are subject to applicable contractual, privacy, security, and access-control requirements.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe below*

Access is determined, approved, and limited, such as role-based access controls, need-to-know determinations, and periodic access reviews. Users are DOI IBC employees with authorized roles. The System Administrator are DOI IBC employees responsible for Box platform security and contractors are subject to applicable security agreements.

Furthermore, Box Enterprise Cloud Content Collaboration Platform user access follows a role-based access control (RBAC) model. For example, general users access only their assigned department files. Managers access team-level documents and Box system administrators maintain Box platform security, but do not have direct access to user files.

2. What data protection policies apply to cloud-based PII storage?

Box, Inc. maintains a FedRAMP authorization for its cloud service product. FedRAMP is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services is responsible for all audits of its platform. Box uploads its vulnerability scans to a continuous monitoring file for the agency, enabling the DOI Information System Security Officer (ISSO) to verify these vulnerability scans.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

To mitigate improper sharing of PII or accidental disclosure, the ISSO enforces data sharing agreements and data encryption in transit and at rest. The system's design and security measures, including MFA, protect data during processing, limiting unauthorized access and potential misuse.

Interior Business Center (IBC) fully complies with NIST and other federal requirements for data security as part

of a formal program of assessment and authorization, and continuous monitoring. The use of the Box Enterprise Cloud Content Collaboration Platform (Box) system is conducted in accordance with the appropriate DOI use policy. Box, Inc. as a company maintains an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed by Box, Inc. on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to Box, Inc security.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

Box logs detail types of events such as login attempts, configuration changes, file access, and use of system utilities. All events are time-stamped with their date and time to provide a temporal context. Information about the terminal identity or location is logged to establish where events occur within the system. Box captures the source of events, including user IDs and network addresses, to identify the origin. Monitoring is strictly for system security and access to logs is restricted.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors may assist with technical support under security agreements. The agreements require compliance with DOI privacy policy. Privacy Act clauses are included.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☒ Other: *Describe Below*

Locked Offices

Technical Controls

☒ Password
☒ Firewall
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)

☒ Encryption
☒ User Identification
☐ Other: *Describe Below*

☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other: *Describe Below*

☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

The Interior Business Center (IBC) Chief of Cybersecurity Group serves as the Box Enterprise Cloud Content Collaboration Platform (Box) Information System Owner (ISO) and the official responsible for oversight and management of the Box security controls and the protection of customer information processed and stored by the Box system. The Information System Owner (ISO) and the Information System Security Officer (ISSO) 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 Box, in consultation with the Office of the Secretary (OS) Associate Privacy Officer (APO).

Customer agency data in Box is under the control of each customer, and the customer 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.

8. What processes are in place for individuals to access their information?

Customer agency data in Box is under the control of each customer, and the customer 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.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Customer agency data in Box is under the control of each customer, and the customer 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.

10. 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 Box Enterprise Cloud Content Collaboration Platform (Box) Information System Owner (ISO) is responsible for oversight and management of the Box security and privacy controls, and for ensuring to the greatest possible extent that Box customer data is properly managed and that all access to customer data has been granted in a secure and auditable manner. The Box Information System Owner (ISO) and ISSO are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with DOI policy and established procedures. The customer data in Box is under the control of the customer. Each customer is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data in accordance with federal and DOI privacy breach response policy.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

Loss, compromise, unauthorized disclosure, or unauthorized access of PII is considered a "security incident". The ISO and all authorized users must report to DOI Cyber Incident Report Council (DOI-CIRC) within one hour of discovery. DOI IBC will follow incident response procedures mentioned in the DOI Privacy Breach Response Plan. Those procedures consist of:

1. Immediate Reporting within one (1) hour of discovery;
2. Containment and mitigation to prevent further loss;
3. Risk Assessment to determine the scope and nature of the breach;
4. Notification, if required;
5. Oversight reporting, if required; and
6. Remediation and prevention to prevent recurrence.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed every three (3) years, in accordance with E-Government Act of 2002, or whenever major changes occur to the system’s technology, data, or operations that could affect privacy risks.