



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:	LeasePro
System or Project Acronym:	LeasePro
Bureau or Office:	Bureau of Indian Affairs (BIA)
Date Signed:	August 7, 2026
System Operational Status:	Development

Point of Contact

Name:	Melissa Allen
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

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

LeasePro supports the Office of Tribal Leases in administering the section 105(l) lease program under the Indian Self-Determination and Education Assistance Act (ISDEAA). The system provides a centralized platform for managing agreements through which the Bureau of Indian Affairs reimburses Tribes and Tribal Organizations for eligible facility costs associated with carrying out approved programs, functions, services, or activities.

The purpose of LeasePro is to manage the full lifecycle of section 105(l) lease applications and renewals, from initial submission through review, approval, funding coordination, and post-award administration. LeasePro enables Tribes and Tribal Organizations to submit applications and supporting documentation electronically and allows authorized Indian Affairs personnel to review submissions, verify information, coordinate required approvals, track application status and milestones, and maintain the records associated with each lease.

By consolidating these activities into a single system, LeasePro replaces manual and fragmented processes, supports consistent processing across the program, improves visibility into the status of lease actions, and provides the Office of Tribal Leases with a reliable record of applications, decisions, approvals, and ongoing lease administration.

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.

LeasePro GRC Registration Number: BIA – 0041- MAJ, UII: 010-000002928

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

The information collected and used in connection with Tribal facility leasing, development, and program operations—including facilities such as domestic-violence shelters and family-protection centers—is authorized under the ISDEAA, 25 U.S.C. § 5324(l). This law provides Tribes with self-determination authority to approve and manage leases of Tribal trust land for Tribal purposes. For example, a Tribe may lease a piece of Tribal trust land to a Tribal department or Tribal nonprofit organization for the construction and operation of a domestic violence shelter, and the lease can be approved entirely under Tribal law and Tribal leasing procedures rather than requiring separate Secretarial approval.

Additional authority comes from the Indian Child Protection and Family Violence Prevention Act (Public Law 100-297), which supports programs designed to prevent and respond to family violence and protect Indian children, and from regulations at 25 C.F.R. §§ 900.69–900.74, which require certain information to be submitted when Tribes carry out self-determination contracts and related agreements. The Indian Employment, Training and Related Services Demonstration Act of 1992 (Public Law 102-477) also allows Tribes to coordinate and integrate social service programs, which may involve sharing program information to support service delivery.

LeasePro's collection and use of personal information are authorized under the Privacy Act of 1974, which allows federal agencies to maintain records about individuals when the information is relevant and necessary to carry out an agency function. LeasePro uses personal information only as needed to administer federal leasing activities and does so in accordance with all applicable laws, regulations, and DOI requirements for records management, privacy protection, and proper system use.

These authorities collectively support the limited collection and maintenance of personal, organizational, and operational information necessary to administer lease agreements, oversee program operations, and meet reporting requirements under the oversight of BIA.

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

This system maintains records related to Tribal Governments, not individuals. While some PII is collected, records are not routinely retrieved by personal identifiers. Because the information is not about an individual in a personal capacity and the system does not retrieve records by personal identifier as its organizing method, this system does not constitute a system of records as defined by the Privacy Act. The LeasePro Application does not create Privacy Act records beyond those generated through its use of Active Directory (AD) for user authentication. For additional information regarding user authentication, please refer to the DOI Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment available on the [DOI Privacy website](#). SORN coverage for records associated with AD authentication is provided under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), as modified at 86 FR 50156 (September 7, 2021). This SORN covers information collected on individuals who require access to Departmental networks, information systems, and email services, including Departmental employees, contractors, students, interns, volunteers, and similar user populations.

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

- ☒ Yes
☐ No

This project involves an information collection that requires OMB approval under the Paperwork Reduction Act (PRA). The collection of information Tribes and Tribal Organizations when they submit lease application packages triggers the PRA.

An OMB Control Number does not yet exist for this information collection, so a new Information Collection Request is being prepared and submitted for approval. The program is consulting with the BIA Information Collection Clearance Officer to ensure the collection complies with the PRA and all other applicable laws. The BIA Information Collection Clearance Officer will coordinate with the DOI Information Collection Clearance Officer to review and approve the PRA submission before it is sent to OMB for approval. Information on the status of BIA information collections to OMB for approval is available on [Reginfo.gov](#), a website produced by OMB and the General Services Administration that provides reliable, transparent information about regulations under development to support effective public participation in the regulatory process.

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

No minor applications or subsystems are hosted on this system.

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 | ☒ Personal Email | ☐ Full or Truncated SSN |
| ☐ Driver's license | ☒ Mailing or home address | ☐ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☐ Biometrics/facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☐ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☐ Personal cell phone number | ☒ Financial information | ☐ Nationality |
| ☐ Username / user ID / acct ID | ☐ IP address / network ID | ☐ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☐ Photos / video / audio | ☐ Health / medical information |
| ☒ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Criminal / disciplinary info | ☐ Military records | ☒ Other: Describe below |

When a Tribe or a Tribal Organization submits a lease package for a facility used to operate a health or social services program, LeasePro uses the name, title, and contact information of the authorized Tribal representative to create the lease record, route the agreement for review and approval, and communicate status updates. The representative's email address is typically organization-related but may be personal in limited cases. This information is collected and maintained only so that IA can communicate and coordinate with the Tribe in its official, organizational capacity. It does not relate to the individual's personal traits, behavior, or circumstances, and it is not used to make any determination about the individual personally.

Although "Tribal ID number" and "Financial information" are checked as categories of data stored in LeasePro, these elements refer to information about the Tribe or Tribal Organization, not personal details about the Tribal representative. Financial records, Tribal identifiers, and related documents are part of the organizational lease package and are used only to evaluate and administer the 105(l) lease.

Additional PII is not requested or stored unless it is specifically required to support lease execution or legal documentation, ensuring that LeasePro collects and uses only the information necessary for program operations.

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

- | | |
|---|--|
| ☐ Individual | ☐ DOI Records |
| ☐ Federal Agency | ☐ Third Party Records |
| ☒ Tribal Agency | ☐ State Agency |
| ☐ Local Agency | ☒ Other: <i>Describe Below</i> |

An attorney may provide information to BIA on behalf of a Tribe. The information is considered to have been collected from the Tribal Government, not from the attorney in their personal capacity.

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

- | | |
|--|--|
| ☒ Paper Format | ☐ Fax |
| ☒ Email | ☒ Telephone Interview |
| ☒ Face-to-Face Contact | ☐ Shared Between Systems: <i>Describe</i> |
| ☐ Website | ☒ Other: <i>Describe</i> |

The LeasePro application is accessed by users through a web interface. Tribes and Tribal Organizations typically submit applications and supporting documentation to BIA via email. They may also provide information to BIA via paper format, face-to-face contact, and telephone. Users upload Microsoft Word, Excel, and PDF files submitted by Tribes and Tribal Organizations, which are integrated through manual data entry. The application then processes this information into the required data elements in accordance with the OTL business rules.

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

The information is collected to administer and manage lease agreements under Section 105(l), including establishing and maintaining lease records, identifying and verifying individuals associated with leases, communicating with representatives, processing lease actions, and supporting oversight, reporting, and compliance activities.

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

The system applies data minimization principles by collecting and using only the specific PII elements necessary to accomplish the intended purpose. Additional personal details are not requested or stored unless they are required to support lease execution, or legal documentation, ensuring PII use is limited to what is necessary for program operations. Access is limited to authorized users based on role and business need.

PII collection requirements are reassessed at least annually during the PIA review cycle to ensure continued alignment with operational needs and to remove any fields no longer required.

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.

PII is shared internally for limited purposes. The BIA Office of Self-Governance is involved in fund distribution and the DOI Office of the Solicitor provides document review. BIA regional offices and Bureau of Indian Education 297-grant awarding officials also participate in fund distribution. OTL and Tribal agency contractors are provided with need-to-know access.

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

The lease serves as the authoritative legal instrument defining roles, responsibilities, and authorized use. As such, the lease functions as the governing document for the relationship and does not require supplementation through a separate Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU).

LeasePro currently has no external system interconnections that require a Service Level Agreement, MOU, MOA, or any other formal interconnection agreement. All services supporting LeasePro are provided through DOI-managed environments, and any future connections to non-DOI identity or access providers would be documented if implemented.

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.*

Tribe or Tribal Organization point of contact information is essential to completing the process of leases. While Tribes and Tribal Organizations must provide PII for a point of contact, they are informed of BIA's use of the information through a Privacy Notice at the point of collection, and data is used only as described in this PIA.

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

☐ Privacy Act Statement:

☐ Other: *Describe Below*

☒ Privacy Notice:

☐ None: *Example - law enforcement cases.*

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

Data within the LeasePro System is retrieved through system-wide search and advanced query capabilities that allow authorized users to locate records across applications, renewals, contacts, documents, and workflow activities. Access to retrieved data is controlled by role-based permissions to ensure users can only view information appropriate to their job responsibilities.

The system's design and operational use organize and retrieve records using system-generated identifiers such as lease application numbers, renewal numbers, and internal record IDs, as well as business identifiers such as Tribal Organization name, facility name, and program or organizational identifiers. Additional retrieval methods include searching by application status, workflow stage, assigned staff member, document title or document

type, and relevant date ranges such as submission date, approval date, or last modified date. These identifiers support efficient location of records needed for processing, review, oversight, and reporting.

Although the system includes a search function capable of retrieving information using contact-level identifiers, including contact person name, business email address, and business phone number, this function is not part of the system's standard operating workflow and is not used as a routine method of retrieving records in the ordinary course of business. The system's retrieval practice, structure, and organizing logic are built around the Tribal entity and facility, not the individual contact. Accordingly, because records are neither maintained about individuals in a personal capacity nor routinely retrieved by personal identifier, this system does not constitute a system of records under the Privacy Act.

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

Any logs that may be generated relate solely to Tribal-level information and administrative processing, not to individual user accounts or PII.

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

Data collected directly from Tribes or Tribal Organizations is presumed to be accurate at the time of submission. Tribes and Tribal Organizations can update their information at any time to ensure it remains accurate. Billing information, such as names and addresses of owners and lessees of irrigable land, is based on information included in legal documents.

Section 4: Data Management and Retention

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

Program records are covered by IA Records Schedules in [Records Group 75](#) (Self-Determination Contract Files, N1-075-88-002) and have been scheduled as permanent records by National Archives and Records Administration (NARA).

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A – Short-term Information Technology Records, 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.

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

The system migrated data from legacy shared-drive repositories and validated the converted data for accuracy. Staff review submissions from Tribes and Tribal Organizations to validate the accuracy and completeness of the information provided. Users upload Microsoft Word, Excel, and PDF documents and diagrams which are combined by manual use entries and then are processed by the application into the necessary data elements that OTL business rules require. LeasePro generates documents using pre-defined OTL templates and produces Microsoft Word and PDF files through Microsoft Dynamics automation.

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

- ☒ Yes
☐ No

All privileged accounts and associated access rights are subject to periodic review and validation in accordance with OTL account management and audit requirements. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. 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 usernames. System administrators and the information system owner have access to these activity reports.

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?

There are several privacy risks associated with the collection, use, retention, and disclosure of PII within LeasePro. IA minimizes these risks by following DOI privacy policies and applying mitigation measures at each stage of the information lifecycle.

Below are the key risks identified for LeasePro, along with associated mitigation strategies documented in the Integrated Risk Register:

- **Risk – Manual data tracking:** Current lease-related PII is tracked and processed through manual workflows. Manual entry increases the likelihood of inconsistent data handling, transcription errors, and lost or misplaced information. Inefficient processes elevate the risk of improper use of information, delayed actions, or incomplete documentation.

Mitigation – IA is acquiring the LeasePro software solution, which will streamline workflows and improve accuracy, consistency, and accountability across all stages of PII handling.

- **Risk – Delays in payment to Tribes:** After a lease is signed, payment to the Tribe must occur in a timely manner. While primarily an operational risk, delayed payments caused by fragmented processes may also increase the amount of PII being re-reviewed, recirculated, or resent between personnel to resolve

discrepancies. This additional handling elevates the risk of exposure or improper use.

Mitigation – IA is working with the AS-IA Office of Budget and Performance Management to address immediate issues. Long-term mitigation includes modernizing the system to automate the LeasePro FED process.

- **Risk – Difficulty transmitting large lease documentation:** Large files often require multiple email transmissions or ad-hoc transfer methods. Increased email traffic and inconsistent file-sharing practices elevate the risk of PII being misplaced, lost, or shared with unintended recipients.

Mitigation – IA will use an approved solution to support secure file sharing until the permanent LeasePro solution is implemented.

- **Risk – Over-collection or collection of unnecessary PII:** There is a risk that IA could collect more PII than is needed to administer a lease, especially when using email-based intake or legacy forms that lack standardized fields. Over-collection increases the amount of sensitive information requiring protection and storage.

Mitigation – IA follows DOI data-minimization requirements and collects only information necessary for lease administration. Submissions are reviewed by staff to ensure relevance and necessity before storage.

- **Risk – Inaccurate, outdated, or improperly used information:** PII submitted by Tribes or Tribal Organizations may be incomplete, outdated, or contain errors. Manual processing increases the risk of transcription mistakes, misrouting, or improper interpretation of data, which could affect decision-making and compromise the integrity of the leasing process.

Mitigation – Staff review submissions for accuracy and completeness. Role-based access controls limit access to authorized personnel consistent with least privilege principles.

- **Risk – Retention of information longer than necessary or storing information inconsistently:** PII may be retained beyond approved retention periods or stored across fragmented repositories such as legacy shared drives. Inconsistent storage increases the risk of unmanaged copies, unauthorized access, and non-compliance with NARA and DOI records requirements.

Mitigation – LeasePro will centralize records within DOI-approved platforms (e.g., SharePoint), reducing reliance on legacy shared drives. Records retention will follow applicable NARA-approved schedules and DOI records management policies.

- **Risk – Unauthorized access or improper sharing of PII:** There is a risk that PII may be accessed or shared by personnel who do not have a validated need-to-know, particularly when information is transmitted through email or stored in shared repositories. Unauthorized access could compromise sensitive Tribal information.

Mitigation – Access to LeasePro requires DOI authentication, with permissions assigned based on user roles and responsibilities. Audit logs track access and activity to support monitoring, oversight, and compliance reviews.

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

N/A

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

☐ Yes: *Provide explanation below*

☒ No

N/A

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

☐ Yes: *Provide explanation below*

☒ No

LeasePro does not include analytical, decision-support, scoring, or evaluative features that assess individuals or derive conclusions about them. All information processed through the system is used solely to administer 105(l) lease agreements and related operational tasks; it does not generate new insights about individuals beyond the information already provided by Tribes or Tribal Organizations.

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

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.*

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

N/A

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

- ☐ Yes
☐ No

N/A

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

- ☐ Yes
☐ No

N/A

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

- ☐ Yes
☐ No

N/A

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

- ☐ Yes
☐ No

N/A

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 | ☒ System Administrator |
| ☒ Contractors | ☒ Other: <i>Describe below</i> |
| ☒ Developers | |

Users are only given access to data based on the “least privilege” principle combined with a “need-to-know” to complete assigned duties. BIA manages user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for Identity Lifecycle Management (ILM). BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards until they depart the DOI. BSAM is used to establish, activate, modify, review, disable user accounts. Federal employee access requires supervisor approval. Contracting Officer’s 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.

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

For the Lease Pro system, all cloud-based storage and processing of PII is governed by DOI privacy and IT security policies and must comply with the Privacy Act of 1974, Federal Information Security Modernization Act, and OMB Circular A-130. The system implements security and privacy controls consistent with NIST SP 800-53 and guidance for protecting PII, and any cloud service supporting the system must be authorized in accordance with Federal Risk and Authorization Management Program (FedRAMP) requirements. These policies require encryption of PII, role-based access controls, audit logging, continuous monitoring, incident response capabilities, and contractual safeguards to ensure the confidentiality, integrity, and availability of PII maintained within the LeasePro system.

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

The LeasePro system monitors and detects unauthorized access, use, and potential data exfiltration through a combination of automated auditing, technical safeguards, and administrative oversight. The system maintains detailed audit logs that record user account creation, modification, disabling, and termination, as well as usernames, logon dates and times, successful and unsuccessful login attempts, files accessed, and changes made to records. These logs enable administrators to identify anomalous behavior, reconstruct security-relevant events, and investigate potential misuse. Firewalls and network security configurations are built into the system architecture, and controls aligned with NIST SP 800-53 and other DOI security policies, are fully implemented to protect against unauthorized access and monitoring. System Administrators regularly review audit logs and user activity to ensure appropriate system use and to detect suspicious patterns that may indicate unauthorized activity or data exfiltration. Any suspected unauthorized access, scanning, or misuse is reported immediately to IT Security for investigation. Access is further protected through role-based permissions assigned according to the principle of least privilege and separation of duties. All users must also agree to DOI Rules of Behavior and complete required privacy and security awareness and role-based training before acquiring system access and annually thereafter to maintain access, thereby reinforcing proper handling of information and supporting early identification and reporting of potential security incidents.

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

The purpose of the LeasePro system is not to monitor individuals; however, user activity within the system is logged to meet DOI security requirements. Audit logs record authorized users' access and actions within the system and may be used to run reports for security reviews or compliance purposes.

In addition to basic access tracking, the system maintains detailed audit logs capturing specific user activity necessary to detect unauthorized access or misuse. System-generated logs may include user account lifecycle events (i.e., account creation, modification, disabling, and termination), authentication activity (i.e., successful and unsuccessful login attempts, logon dates and times), system usage, and submission and document-related actions.

Access to audit information is restricted to authorized personnel, including the Information System Owner (ISO), Information System Security Officer (ISSO), and designated system administrators, who review logs to ensure lawful and appropriate use. Monitoring is performed in accordance with applicable DOI policies, the DOI Rules of Behavior, and role-based access controls that limit information access to users with a valid need to perform their responsibilities.

These controls collectively ensure that user activity monitoring is limited to security, operational integrity, and compliance purposes, and that any access to audit logs is appropriately governed, documented, and restricted.

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

- ☒ Design
- ☒ Development
- ☒ Maintenance

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 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), and FAR 52.239-1, Privacy or Security Safeguards (Aug 1996).

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

Physical Controls

- | | |
|--|---|
| ☒ Security Guards | ☐ Cipher Locks |
| ☐ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☐ Safes |
| ☒ Secured Facility | ☐ Combination Lock |
| ☐ Closed Circuit Television | ☐ Other: <i>Describe Below</i> |

PII used or accessed by personnel supporting the program is protected by multiple facility-level safeguards:

Security Guards and Secured Facilities: Access to DOI facilities is restricted to cleared individuals. Physical entry requires passing security checkpoints staffed by trained security personnel.

Identification Badges: All personnel must display DOI-issued identification badges when entering or moving within secure areas. Badge access controls ensure only authorized individuals can enter workspaces or secure zones.

Locked File Cabinets: Any physical documents containing PII are stored in locked cabinets within secured office environments to prevent unauthorized access.

These controls collectively limit physical access to PII and ensure that only approved personnel can enter areas

containing sensitive information.

Technical Controls

- | | |
|--|---|
| ☐ Password | ☐ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☐ Virtual Private Network (VPN) |
| ☒ Encryption | ☐ Public Key Infrastructure (PKI) Certificates |
| ☐ User Identification | ☐ Biometrics |
| ☒ Other: <i>Describe Below</i> | |

Multiple technical safeguards are implemented to protect PII in accordance with DOI security and privacy requirements and align with NIST SP 800-53, OMB Circular A-130, and DOI cybersecurity directives:

Firewall: DOI enterprise firewalls restrict network traffic to authorized and trusted sources, preventing unauthorized access and isolating LeasePro within a secure network environment.

Encryption: Data transmitted to or from the system is protected using DOI-approved encryption mechanisms. Encryption ensures that PII remains unreadable to unauthorized users during transmission or storage within supporting environments.

Audit Logging and Activity Monitoring: LeasePro maintains system-level audit logs recording user access, authentication attempts, and actions performed within the system. These logs support DOI's oversight requirements and help detect and prevent unauthorized use while ensuring traceability of user activity.

Secure Configuration: Servers supporting LeasePro follow DOI baseline configuration requirements, including patch management, restricted service accounts, and system configuration hardening to reduce vulnerabilities.

Other (PIV Card and Multi-Factor Authentication): Access to LeasePro requires the use of a PIV card and MFA. Users must authenticate using both their government-issued PIV card and an associated PIN or credential, providing a phishing-resistant, two-factor verification mechanism. This ensures that only authorized personnel with validated identities can access systems containing PII. MFA strengthens protection against unauthorized access by requiring two independent authentication factors, even if one factor is compromised.

These technical controls collectively ensure that PII within LeasePro is protected from unauthorized access, disclosure, alteration, and misuse, consistent with DOI's enterprise security architecture.

Administrative Controls

- | | |
|--|---|
| ☒ Periodic Security Audits | ☒ Methods to Ensure Only Authorized Personnel Have Access |
| ☐ Backups Secured Off-site | ☐ Encryption of Backups Containing Sensitive Data |
| ☒ Rules of Behavior | ☒ Mandatory Security, Records and Privacy Training |
| ☒ Role-Based Training | ☒ Regular Monitoring of Users' Security Practices |
| ☒ Other: <i>Describe Below</i> | |

Administrative safeguards ensure users handle PII appropriately and comply with DOI policies:

- **Periodic Security Audits:** Regular audits verify compliance with DOI privacy, records management, and cybersecurity requirements.
- **Access Restrictions Based on Need-to-Know:** Access to PII is granted only to authorized personnel whose duties require it. RBACs restrict permissions to the minimum necessary.
- **Rules of Behavior:** All users must sign and comply with DOI Rules of Behavior, affirming their responsibility to protect PII and follow security protocols.
- **Mandatory Privacy, Security, and Records Management Training:** Personnel with access to LeasePro must complete annual training on privacy requirements, cybersecurity practices, and proper handling of sensitive data.
- **Role-Based Training:** Personnel are assigned to defined system roles—such as Standard User, Management User, Administrator, and Read-Only User—and must complete role-based privacy and security training appropriate to those responsibilities.
- **Continuous Monitoring and Incident Response Procedures:** System activity is monitored as part of DOI cybersecurity oversight. Incident reporting requirements ensure timely notification and mitigation of any suspected or confirmed privacy breaches.

These controls ensure PII is handled in accordance with federal privacy laws, DOI policies, and established best practices.

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

Although LeasePro is not itself a Privacy Act system of records, authentication and user account information are covered under an existing SORN. Any Privacy Act complaints involving those records are processed in accordance with DOI's Privacy Act procedures.

Tribes and Tribal Organizations may submit general privacy complaints regarding the handling of information they provide to BIA, including concerns about accuracy, misuse, inappropriate access, or broader privacy impacts to their organizations. These complaints are accepted through established oversight processes and are reviewed to ensure the proper protection and stewardship of Tribal data.

All complaints are received and initially reviewed by the ISO. The ISO coordinates with the ISSO, bureau system managers, and the Privacy Officer to review the complaint, assess the issue, and determine appropriate corrective actions or responses. This process also applies to Privacy Act requests for notification, access, amendment, or redress, ensuring that individuals' and Tribal entities' privacy concerns are addressed in a timely and compliant manner.

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

Tribes and Tribal Organizations may request access to information they previously submitted to the program by contacting the program directly through its designated communication channels. Upon receiving a request, the program will verify the identity and authority of the requester to ensure that the information is being provided to an authorized Tribal representative. Verification may include confirming the individual's role, validating contact information against records on file, or requesting written confirmation from the Tribal Government or organization. Once verification is complete, the program will provide the requested information in a secure and appropriate manner.

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

Tribal representatives may request correction of information submitted to the program by contacting the program through its designated communication channels. Upon receiving a correction request, the program will verify the identity and authority of the requester to ensure they are an authorized representative of the Tribe or Tribal Organization. Verification may include confirming the individual's role, validating contact information against program records, or requesting written confirmation from the Tribal Government or organization. Once verification is complete, the program will work with the Tribal representative to review the identified inaccuracies and update the information in a timely and accurate manner.

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 LeasePro System 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, ISSO and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the DOI Computer Incident Response Center (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 Privacy Officer.

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?

For the LeasePro system, in the event of a suspected or confirmed privacy breach involving PII, immediate actions are taken to contain the incident, prevent further unauthorized access or disclosure, and preserve evidence. The incident is promptly reported to the appropriate DOI incident response teams and DOI-CIRC in accordance with the DOI Privacy Breach Response Plan. Security and privacy officials coordinate with LeasePro staff and contractors to investigate the incident, assess the scope and impact, and determine the type of information involved. Mitigation actions may include isolating affected systems, resetting credentials, applying patches, and implementing additional safeguards. Notifications to affected individuals and external oversight entities are coordinated and approved by authorized DOI officials in consultation with privacy officials. When notification is required, affected individuals are informed of the nature of the breach, the types of information

involved, steps they can take to protect themselves, and what the Department is doing to mitigate harm and prevent future incidents. Additional services, such as credit monitoring, may be provided when appropriate. All breach handling activities are documented and conducted in accordance with federal and DOI breach response policies.

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

For the LeasePro Cloud system, this PIA is reviewed annually through the Privacy Threshold Analysis process and updated when substantive changes affect the assessment's accuracy, scope, privacy risk posture, or legal sufficiency. Updates are coordinated with DOI privacy officials and the LeasePro program office to ensure continued accuracy and compliance.