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: Alaska Land Information System
Bureau/Office: Alaska State Office
Date: 09/17/18
Point of Contact:
Name: Suzanne S. Wachter
Title: Bureau Privacy Officer
Email: swachter@blm.gov
Phone: 202-912-7178
Address: swachter@blm.gov

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The Department of the Interior's (DOI)'s Bureau of Land Management (BLM) has the responsibility for maintaining the land and mineral records for the United States - what today amounts to more than a billion records. The BLM has also been designated by OMB Circular A-1, revised August 19, 2002, as the lead agency for:

Federal Land Ownership Status:
The Alaska Land Information System (ALIS) provides the BLM with an operational system for

electronic management of federal land ownership records.

Public Land Conveyance (patent) Records:
ALIS, through its Land Documents subsystem, provides the BLM with operational systems for electronic management of public land conveyance records. ALIS is a relational database management system and is BLM Alaska's official land and mineral case record system. ALIS is an integrated, centralized system that contains case record data for all land and mineral actions including conveyances, withdrawals, mining claims, mineral leases, oil & gas leases, grazing permits, right of ways (ROWs) and realty actions. The system stores, manages and distributes information about individual cases, customers (private, corporate, and governmental), actions that take place on a case, land descriptions, rights and interests to the lands and relevant financial data. ALIS supports the Alaska Land Transfer Program, management of mining claims, oil and gas leases, resources management, recreation management, land use planning, and land ownership. Digital images of case related documents such as Master Title Plats, Survey Plats, Survey Field Notes, Easement Diagrams, and Conveyance Documents are integrated with this system. ALIS has the capability of providing up to date land status and ownership information based upon data connections within the system. The system has extensive reporting capabilities and provides data supporting GIS/mapping activities. This is the system used by BLM Alaska to support the transfer of land and mineral rights and interests from the Federal Government to other entities in accordance with the Alaska Statehood Act, Alaska Native Claims Settlement Act (ANCSA), Alaska National Interest Lands Conservation Act (ANILCA), and the Alaska Native Allotment Act. This system has been in an operations and maintenance status since 1992.

C. What is the legal authority?

The BLM established this system of records to provide and maintain a lands and minerals database to be used at the BLM-Alaska facilities under multiple legal authorities, including 43 U.S.C. 1601 (Alaska Native Claims Settlement Act), 43 U.S.C. 1701 (Federal Land Policy and Management Act), 42 U.S.C. 4601 (Uniform Relocation Assistance and Real Property Acquisition Policies Act), and the various statutes as listed in the regulations in chapter II of tile 43 of the Code of Federal Regulations.

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*

010-000000085 ALIS System Security Plan signed by TM_RW.pdf

☐ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
ACRES	ACRES is the internal web reporting system for ALIS. It allows BLM employees to retrieve cases by area, case type, customer, case status. case activity, survey id, patent number, etc.	Yes	ACRES is a read-only reporting system for ALIS. It contains customer names and addresses
External ACRES	External ACRES is the web reporting system available for public use. It allows the public to view case abstracts for the cases in ALIS. Cases can be retrieved by customer, surveyid, patent and township.	Yes	External ACRES is a read-only reporting system for ALIS that is available on the internet. ACRES reports contain BLM Alaska case information. Reports include native, state and private land conveyance cases, as well as, leases, permits, federal mining claims, easements, etc. Customer name is the only PII available, and addresses are filtered out.
Historical Index	HISTORICAL INDEX contains a record of all federal actions on each township in Alaska, for example, federal withdrawals and land patents and valid selections. The system consists of a data maintenance module and a reporting module which is available on ACRES and External ACRES.	No	N/A

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Land Documents System	Land Documents System - MTP, Conveyance Document, and Survey Plat Image Retrieval – This system contains images of the Master Title Plats (MTPS), conveyance documents such as patents and Interim Conveyances, and images of BLM survey plats.	No	N/A
Spatial Data Management System	SDMS (Spatial Data Management System) – Report module – Available on the public website, used by both internal and external customers. This module provides spatial reports for many types of BLM data including collected survey parcels, generalized land status information extracted from ALIS data.	No	N/A

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 about individuals are covered by **LLM-32 Lands & Minerals Authorization Tracking System,** 56 FR 5014, February 7, 1991; Modification published 73 FR 17376, April 1, 2008, which may be viewed at https://www.doi.gov/privacy/blm_notices. The LLM-32 SORN is currently being revised to provide updated content for the system and incorporate new Federal government-wide requirements in accordance with OMB Circular A-108.

☐ N o

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

☒ Yes: *Describe*

OMB Control Number 1004-0009, Land Use Application and Permit (43 CFR 2920), Expiration 31 March 2020

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*
The system contains names, addresses, interest relationships and percent interest for Individuals, government entities, entrepreneurs, and other business entities holding permits, leases, or other authorizations to use public lands.

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
☐ Website
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

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

The information in ALIS is abstracted from DOI/BLM Federal records and documents such as land use applications that are contained in DOI/BLM case files. The information in the Federal records is

provided by the public, State of Alaska, or Federal Agencies in the process of their doing business with the BLM. Some of applicants are individuals. BLM employees perform the data extraction and data entry into ALIS. The intended use is to create a fair digital representation of the information contained in the federal record. Individual names and address are collected for the purpose of establishing a public record of the transfers of title to and from the Federal Government and authorized uses of public lands in accordance with the Alaska Statehood Act, Alaska Native Claims Settlement Act (ANCSA), Alaska National Interest Lands Conservation Act (ANILCA), the Alaska Native Allotment Act and other federal regulations.

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

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

ALIS supports the Alaska Land Transfer Program, management of mining claims, oil and gas leases, resources management, recreation management, land use planning, and land ownership. Digital images of case related documents such as Master Title Plats, Survey Plats, Survey Field Notes, Easement Diagrams, and Conveyance Documents are integrated with this system. ALIS has the capability of providing up-to-date land status and ownership information based upon data connections within the system. The system has extensive reporting capabilities and provides data supporting GIS/mapping activities which is conducted by other BLM programs. This is the system used by BLM Alaska offices and other headquarter BLM offices to support the transfer of land and mineral rights and interests from the Federal Government to other entities in accordance with the Alaska Statehood Act, Alaska Native Claims Settlement Act (ANCSA), Alaska National Interest Lands Conservation Act (ANILCA), and the Alaska Native Allotment Act. Other DOI agencies may also use the information contained within ALIS for conducting business with BLM.

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

Bureau of Indian Affairs, National Park Service, US Fish and Wildlife Service access the external ACRES system where name is released and address is filtered from the digital record. Data is used by these agencies in the course of their land management responsibilities.

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

Any federal agency can access the external ACRES system where name is released and address is filtered from the digital record. Data is used by these agencies in the course of their land management responsibilities. Records may be shared with the Department of Justice to provide support in cases where there is litigation or court proceedings, and may be shared with other Federal agencies as authorized under the routine uses outlined in the LLM-32, Land & Minerals Authorization Tracking System, system of records notice.

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

Any Tribal, State or Local agency can access the external ACRES system, as members of the public, where name is released and address is filtered from the digital record. Data is used by these agencies in the course of their land management responsibilities.

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

Information may also be shared with contractors employed by BLM as support.

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

Any member of the public can access the external ACRES system where name is released and address is filtered from the digital record. Data is used by these entities in the course of reviewing land management activities.

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.*

Information is obtained primarily from the Land Use Application and Permit form for the purpose of establishing a publicly accessible record of transfers of title to and from the Federal Government and authorized uses of public lands. Individuals voluntarily provide information when they complete and submit applications, and have the opportunity to decline or consent to the use of their information.

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

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

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

A Privacy Act Statement is included on the Land Use Application and Permit form used by the program to collect information, and is posted on the official BLM website.

☒ Privacy Notice: *Describe each applicable format.*

Notice is also provided through the publication of this privacy impact assessment and the LLM-32, Land and Minerals Authorization Tracking system of records notice, which may be viewed at Privacy Policy / BLM-32 Lands & Minerals Authorization Tracking System

☐ Other: *Describe each applicable format.*

☐ None

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

Data can be retrieved by customer name, customer number, survey type/number, Claim name, or Land Document number. Name and address are the only PII received from the customer and are required to conduct business with the BLM.

I. Will reports be produced on individuals?

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

Information in the system has been collected for the purpose of establishing a publicly accessible record of transfers of title to and from the Federal Government and authorized uses of public lands. ALIS reports on all customers, some of whom are individuals. Internal BLM customers have access to the publicly accessible record, whereas external customers can only electronically access customer name and no other personally identifiable information.

☐ No

Section 3. Attributes of System Data

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

Data is not collected from alternate sources other than DOI/BLM records that are publicly accessible record of transfers of title to and from the Federal Government and authorized uses of public lands. BLM land and mineral adjudication staff verify accuracy of data extracted from publicly accessible physical case records and application forms prior to entry into ALIS and upon closure of case files.

B. How will data be checked for completeness?

The data verification and quality control process documents the accuracy or factuality of data through a comparison to the source data. Data sampling is a means of checking selected portions of data in a database to determine its quality level. Error detection involves comparing the data against the source documentation and comparing it with established data standards to determine if the data is in conformance with the standards. Documentation of the sampling and error detection activities consists of the date of action, steps taken, name of parties involved, summary of errors detected with an analysis of the errors, and the date corrective actions are taken. Records may be audited in the event of litigation,

the records in this system may be required as evidence that the system is trustworthy, accurate, and reliable.

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

The current data model is the Alaska Land Information System physical data model. Data elements in ALIS are described in the ALIS Data Dictionary maintained as part of the BLM Alaska State Data Dictionary. The data contained in ALIS reflects the physical case file. If and when data is changed or added to the case file, that data is changed or added in ALIS. This is done by BLM adjudicators and legal instruments examiners, as part of their assigned duties.

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

Records maintained in ALIS are covered by BLM records retention schedule under DAA-0049-2013-0004-0001, which was approved the National Archives and Records Administration (NARA). The ALIS records are permanent and the disposition authority states to transfer a copy along with a public use version to NARA, in accordance with NARA transfer instructions applicable at the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession.

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

The ALIS records are permanent and the disposition authority states to transfer a copy along with a public use version to NARA immediately, in accordance with NARA transfer instructions applicable at the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession.

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.

Users do not have full access to all data in the system. Access levels are established and pre-approved based on business needs. Information within the system are generally considered public data and is made available to the public at their request. However, some data related to certain case types, such as Native Allotments, or Law Enforcement or cultural resource data that are part of a case file must be reviewed by the BLM-Alaska FOIA/Privacy Officer prior to release. The same process is followed for the hard copy case file for those select case types.

Personnel security controls are implemented to ensure that persons are appropriately screened for the information to which they will be allowed to access, that they receive no access outside their need to know, that appropriate procedures are in place for the establishment and closure of user accounts, and

that users are aware of their responsibilities to protect the data to which they have access.

Only those employees (i.e. system administrators) that need access to server systems have root/administrator access privileges. All positions have been evaluated for sensitivity and all Federal and contract employees with root/administrator access to these systems have had background investigations performed under contract by the Personnel Office. All system users are granted access to the systems based on the principle of least privilege.

Five levels of access are built into this application and are based on least privilege principles, with different levels for case processing updates, BLM Public Room staff data entry, ad hoc queries and special processing, BLM Data Administration staff, and database administrator functions. Access is granted to specific employees based upon a completed user registration request form which requires signed supervisor approval. This completed form is kept on file in the Computer Operations Center. IT staff assigns system, host, and user access based upon the requested access level. When employees are terminated or move from BLM Alaska, their login IDs on this system are revoked. Passwords must be changed every 90 days. Users whose account passwords have not been changed before 90 days must change their password upon login. A password grace time parameter that defines this period of grace time (7 days), once the grace time has passed, the account status is set to 'expired.' The administrator will lock and/or terminates the account after the 7 day grace period expires.

There is a moderate privacy risk due to the type and volume of personal information maintained in the system. Information collected and used is limited to the minimum required to perform the purpose and functions of the system. ALIS supports the Alaska Land Transfer Program, management of mining claims, oil and gas leases, resources management, recreation management, land use planning, and land ownership. Digital images of case related documents, such as Master Title Plats, Survey Plats, Survey Field Notes, Easement Diagrams, and Conveyance Documents are integrated with this system. ALIS has the capability of providing up to date land status and ownership information based upon data connections within the system. The system has extensive reporting capabilities and provides data supporting GIS/mapping activities. This is the system used by BLM Alaska to support the transfer of land and mineral rights and interests from the Federal Government to other entities in accordance with the Alaska Statehood Act, Alaska Native Claims Settlement Act (ANCSA), Alaska National Interest Lands Conservation Act (ANILCA), and the Alaska Native Allotment Act.

There is a risk that individuals may gain unauthorized access to the information in the system. System security controls are in place to prevent access by unauthorized individuals to sensitive information. ALIS is classified as FISMA moderate and has all of the required system security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, ALIS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses of authorized users, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct "need to

know" certain information contained in the system. All end-users have an individual password and ID that is issued by the ALIS application steward. All new users will receive training on the use of the system. All DOI employees must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel, with supervisor approval, that have an official need-to-know to perform their job duties. Access to information is role-based and is only granted on a need-to-know basis, and requires DOI credentials. Accounts are reviewed annually to ensure that only authorized personnel have systems logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing the system must acknowledge the rules of behavior prior to each login. The System Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, etc. Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by the system. The Oracle Database automatically locks any user account following 5 invalid log-in attempts.

There is a risk that information is maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected has intentionally been limited; only the minimal amount of data needed for identification purposes is maintained and used by the system to support the BLM mission. Records in this system are related to the management of mining claims, oil and gas leases, resources management, recreation management, land use planning, and land ownership and have historical value. These records support the transfer of land and mineral rights and interests from the Federal Government to other entities in accordance with the Alaska Statehood Act, Alaska Native Claims Settlement Act (ANCSA), Alaska National Interest Lands Conservation Act (ANILCA), and the Alaska Native Allotment Act. Due to their value, these records have a permanent records retention and all records are transferred to NARA.

There is a risk that an application may be denied based on the submission of inaccurate information. All information is obtained directly from the applicant so is presumed to be complete and accurate. Any inaccurate information provided by the applicant may be corrected during user validation procedures or by the applicant themselves.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA and the BLM Alaska Land Information System notice, and the Privacy Act statement provided on the application and the official BLM website.

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*

ALIS provides BLM employees and customers with a centralized source of land status information such as ownership, surface management agency, use authorizations, and segregation. Information in the system has been collected for the purpose of establishing a publically accessible digital record of transfers of title to and from the Federal Government and authorized uses of public lands.

☐ 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?

ALIS does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

Audit logging is used for purposes such as tracking successful and unsuccessful attempts to access the system and any unauthorized changes to security configurations as well as other potential security violations.

Database integrity is validated by data entry subroutines that snopcan for discrepancies and completeness. Numerous validation tables are used to validate entered data before updates to the database are allowed. Users can 'lock' Land and Actions records to prevent unwanted changes to audited and verified cases. An audit trail is maintained for each update, insert, and delete to the database.

Database entries are compared to validation tables where appropriate. These validation tables are maintained by BLM Alaska Data Management section. A statewide Data Administration Workgroup is composed of knowledgeable ALIS representatives from each field office and division of BLM Alaska. This group reviews requests for updates to these validation tables. Requests to update validation tables must be made in writing.

Data are also reviewed by data auditors where appropriate. These data auditors can lock data they have reviewed. These locks may only be unlocked by a user with the same access-level or above.

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*
Anyone may access the external ACRES system where name is released and address is filtered from the digital record.

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

Users do not have full access to all data in the system. Access levels are established and pre-approved based on business needs. Information within the system are generally considered public data and is made available to the public at their request. However, some data related to certain case types, such as Native Allotments, or Law Enforcement or cultural resource data must be reviewed by the BLM-Alaska FOIA/ Privacy Officer prior to release. The same process is followed for the hard copy case file for those select case types. Anyone may access the external ACRES system where name is released and address is filtered from the digital record.

Personnel security controls are implemented to ensure that persons are appropriately screened for the information to which they will be allowed to access, that they receive no access outside their need to know, that appropriate procedures are in place for the establishment and closure of user accounts, and

that users are aware of their responsibilities to protect the data to which they have access.

Only those employees (i.e. system administrators) that need access to server systems have root/administrator access privileges. All positions have been evaluated for sensitivity and all Federal and contract employees with root/administrator access to these systems have had background investigations performed under contract by the Personnel Office.

All system users are granted access to the systems based on the principle of least privilege. Five levels of access are built into this application and are based on least privilege principles, with different levels for case processing updates, BLM Public Room staff data entry, ad hoc queries and special processing, BLM Data Administration staff, and database administrator functions. Access is granted to specific employees based upon a completed user registration request form which requires signed supervisor approval. This completed form is kept on file in the Computer Operations Center. IT staff assigns system, host, and user access based upon the requested access level. When employees are terminated or move from BLM Alaska, their login IDs on this system are revoked.

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?*

☒ No

No, however, contractors involved in ALIS maintenance do not directly access the ALIS data entry system. Their access is tightly controlled and then only through a BLM system developer that actually performs the system maintenance.

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*

☒ No

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

ALIS does not provide any capability for monitoring individual members of the public. However, audit

logging is used for security purposes such as username, date and time of access, tracking successful and unsuccessful attempts to access the system, and any unauthorized changes to security configurations as well as other potential security violations.

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

Secure terminals, passwords, access control lists, and firewalls provide protection within the database. All activity on the system is continuously monitored and audit logging is enabled.

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*
Offsite backup is encrypted and held within secure facility.

(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 BLM Alaska State Director serves as the ALIS Information System Owner and the official responsible for oversight and management of the ALIS security controls and the protection of information processed and stored by ALIS. The Information System Owner 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 in ALIS. The Information System Owner and System Manager are 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 BLM 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 BLM Alaska State Director has responsibility 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 ALIS Information System Owner and the Information System Security Officer 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 BLM Associate Privacy Officer.