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: Rangeland Administration System (RAS)
Bureau/Office: Bureau of Land Management
Date: December 16, 2022
Point of Contact:
Name: Catherine Brean
Email: blm_wo_privacy@blm.gov
Phone: 830-225-3459
Address: BLM, IRM, DOI National Operations Center, Bldg. 50, Denver, Colorado 80224

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 Rangeland Administration System (RAS) application provides grazing administrative support and management reports to field offices and acts as an automatic calendar for issuance of thousands of applications and authorizations per year. It also creates approximately 30,000 bills per year and passes information to the Collection and Billing System (CBS) for tracking, collecting and distribution of grazing receipts. Data is also used for BLM Publication: "Public Land Statistics."

Internal users (authenticated) process authorizations of the use of public land for grazing purposes, issuance of bills for such use, and record the results of monitoring activities related to managing the use of public lands for grazing. The RAS provides the ability to record and track status of Allotments and Pastures for livestock grazing, the authorizations granted for such purposes, and renewals and transfers of such authorizations; verifying the completion of National Environmental Policy Act (NEPA) activities in ePlanning; the issuance, re-issuance, or cancelation of bills for livestock grazing; providing data for national reporting capability to the Oracle Business Intelligence Enterprise Edition (OBIEE) system to satisfy the full business needs/program requirements.

The RAS is an internal application, with several sub-systems: a geospatial data reviewer (RAS GIS Data Reviewer), a geospatial data reporter (RAS GIS Data Reporter), and a keystore. The GIS Data Reviewer has components and data hosted by the BLM Geospatial Business Platform (GBP) and application components hosted by RAS and is an internal application for the purposes of reviewing and improving the quality of the Range Program's geospatial data (Allotment and Pasture polygons). The GIS Data Reporter has components and data hosted by the BLM GBP and application components hosted by RAS and is an internal application for the purposes of viewing RAS data spatially in conjunction with the Range Program's geospatial geometry. The keystore is an internal application that encrypts the passwords associated with service accounts that are necessary for the operation of the RAS information system. The privacy risks of these subsystems will be addressed in this PIA.

C. What is the legal authority?

Taylor Grazing Act of 1934 43 U.S.C. § 315
Federal Land Policy Management Act of 1976 43 U.S.C. § 1701 et seq
Oregon & California Railroad Revested Lands Act 43 U.S.C. § 1181f
Public Rangelands Improvement Act of 1978 43 U.S.C. § 1901 et seq

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

UII Code: 010-000000164, SSP Title: System Security and Privacy Plan for Rangeland Administration System

☐ 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.*
RAS GIS Data Reviewer	Review and verify the geometry of spatial features belonging to the grazing program	No	N/A
RAS GIS Data Reporter	View RAS data in conjunction with the geometry of spatial features belonging to the grazing program	Yes	View Operator Names and Mailing Addresses (business or home) associated with grazing similar to the public reports
RAS Keystore	Encrypts the passwords for service accounts used within the RAS system	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes:

RAS is covered under INTERIOR/LLM-2, Range Management System,75 FR 82061 (December 29, 2010), modification published 86 FR 50156 (September 7, 2021). LLM-2 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. DOI SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes

Data is input into this information system using forms requiring OMB approval and assigned OMB Control Numbers. Information collection requirements contained in subparts 4120 and 4130 of Group 4100 have been approved by the Office of Management and Budget under 44 U.S.C. 3507 and assigned clearance numbers 004–0019 and 004–0041.

OMB Control Number: 1004-0019, Grazing Management: Range Improvements Agreements and Permits (43 CFR subpart 4120); Expiration March 31, 2023

- Form 4120-6, Cooperative Range Improvement Agreement
- Form 4120-7, Range Improvement Permit

OMB Control Number: 1004-0041, Authorizing Grazing Use (43 CFR subparts 4110 and 4130); Expiration April 30, 2024

- Form 4130-1, Grazing Schedule-Grazing Application
- Form 4130-1a, Grazing Preference Application and Preference Transfer Application (Base Property Preference Attachment and Assignment)
- Form 4130-1b, Grazing Application Supplemental Information
- Form 4130-3a, Grazing Application
- Form 4130-4, Application for Exchange-of-Use Grazing Agreement
- Form 4130-5, Actual Grazing Use Report

☐ No

Section 2. Summary of System Data

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

☒ Name
☒Citizenship
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Group Affiliation
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

The BLM's public website (http://www.blm.gov/ras/) provides information about grazing administration on the National System of Public Lands, including names and addresses of all grazing permit and lease holders who graze livestock on these lands, and phone numbers for business entities. This information is provided in consideration of a United States District Court, District of Idaho decision in Case No. CV 09-482-CWD. In that case, the Court found that there

was substantial public interest in understanding the scope of the grazing and rangeland program, including knowing how many individuals or entities graze cattle on public lands, as well as the size and scope of their operations, and that this public interest outweighed the permit holders' privacy interest in their names, addresses and authorization numbers. Other information contained within the system may be the BLM assigned case file number and operator number; lien holder's name and address; authorized representative's name, address and phone number and name of persons or businesses such as realtors or consultants, representing the grazing permittee. Form 4130-1b, Grazing Application Supplemental Information requires an additional qualification statement that documents whether the applicant meets requirements, besides owning or controlling base property, to qualify for grazing use on public land. The applicant must declare they are either: 1) a United States citizen, (or, has properly filed a valid declaration of intention to become a citizen or a valid petition for naturalization); 2) a group or association authorized to conduct business in the State in which the grazing use is sought, or 3) a corporation authorized to conduct business in state in which the grazing is sought. BLM requires all relevant information requested on any of the application forms be provided so they can determine if an applicant meets all the qualifications.

BLM employees and contractors use their government issued Personal Identity Verification (PIV) authenticated through the Enterprise Active Directory (AD). The system collects the user's name, official email address, username, date of last login, and role or access levels for authorized users.

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:

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:

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

The PII is collected so that BLM staff may contact the individual who has submitted an Expression of Interest (EOI) or is conducting business with the BLM to:

- Request additional information, such as documentation needed to process the EOI request, grazing bills, or authorization management.
- Notify the individual when the requested lands are unavailable for grazing.
- Report status of EOI submission(s), authorization renewal(s) or transfer(s).
- Notify the individual regarding compliance with the terms of grazing authorization(s) resulting from monitoring activities.
- Notify the individual about payment status resulting from the authorization of grazing.

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

☒ Within the Bureau/Office: Within DOI, BLM staff with access to RAS use this data to contact applicants and permittees/lessees to determine the availability of the relevant lands for grazing and whether an application to graze public lands for grazing should be granted, notify individuals when unauthorized livestock are on public land, and monitor grazing use to the extent it may be granted. Data is also shared for national reporting capability to the BLM Oracle Business Intelligence Enterprise Edition (OBIEE) system to satisfy the full business needs/program requirements. It also creates approximately 30,000 bills per year and passes information to the BLM Collection and Billing System (CBS) for tracking, collecting and distribution of grazing receipts.

☐ Other Bureaus/Offices:

☒ Other Federal Agencies: To Federal agencies to administer duties that directly relate to livestock grazing on BLM administered public lands and provide transparency on individual permittees who hold livestock grazing permits on BLM administered public lands. Also, to the Department of the Treasury to recover debts owed to the United States.

☒ Tribal, State or Local Agencies: To tribal and local governmental entities, businesses, organizations, associations, and individuals to administer duties that directly relate to livestock grazing on BLM administered public lands and provide transparency on individual permittees who hold livestock grazing permits on BLM administered public lands.

☒ Contractor: Contractors perform maintenance and enhancements on the system and provide customer support to BLM personnel. The data is used as part of the routine operations and maintenance to validate system performance. Use in non-production environments for analysis

and reproduction of out of bounds behavior (software defects). Contractor staff will be required to undergo background checks as defined by BLM policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system.

☒ Other Third-Party Sources: Disclosures may be made to third parties when authorized and necessary to perform official functions of BLM, as outlined in the routine uses in INTERIOR/ LLM-2, Rangeland Management System, 75 FR 82061 (December 29, 2010), modification published 86 FR 50156 (September 7, 2021). Commercial interests, such as hunting guides, outfitters, energy and minerals developers, and right-of-way applicants, or their representatives, whose activities are likely to affect the grazing permittee's management of livestock or maintenance or use of range improvements and who require the information in order to communicate, consult with or coordinate activities with the grazing permittee. The BLM's public website (http://www.blm.gov/ras/) provides information about grazing administration on the National System of Public Lands, including names and addresses of all grazing permit and lease holders who graze livestock on these lands, and phone numbers for business entities.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: Submission of the requested information for the rangeland resources grazing application process is voluntary. However, individuals must share the requested PII with BLM to receive communications and essential bills in exchange for usage of public lands for livestock grazing and is necessary to obtain, or retain, the benefit of a permit or authorization. Individuals can decline to provide the information however, failure to submit all of the requested information or to complete one of required forms may result in the rejection or denial of the application. The effect of not providing information is addressed within the Privacy Act statement on all of the applicable BLM forms utilized for this program.

☐ No:

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

☒ Privacy Act Statement: The BLM forms identified in 1.H above contain a Privacy Act statement.

☒ Privacy Notice: Notice is provided through the publication of this privacy impact assessment and the INTERIOR/LLM-2, Rangeland Management System, 75 FR 82061 (December 29, 2010), modification published 86 FR 50156 (September 7, 2021). DOI PIAs and SORNs may be viewed at https://www.doi.gov/privacy/pia and https://www.doi.gov/privacy/sorn.

☒ Other: Both the BLM Natural Resources site used for informational and instructional purposes, and the Electronic Forms site, where applicable forms are available for download, contain a hyperlink to the DOI Privacy Policy page.

☐ None

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

The BLM staff will be able to search for authorizations held by members of the public and the operator's name can be a filter on lists of data in the system. However, the search feature does not allow the BLM staff to search on an individual's mailing address, home phone number, cell phone number, or e-mail address. PII other than name is specifically excluded from the allowable search parameters. By design, the most common searches are not based on PII. The search parameters most frequently used to locate records in the system are Authorization Number, Allotment Number, Bill Number, and other Authorization or Land Attributes, such as type of authorization, effective and expiration dates of the Authorization, grazing dates, type of grazing, kind of livestock grazed, and land status.

I. Will reports be produced on individuals?

☒ Yes

Reports are available internally to BLM staff and a smaller subset of reports are available externally to the public. The reports are generated from the information in RAS. The purpose of the information in RAS is to (1) maintain an orderly record of grazing permittee information, allotment information, historical allotment or grazing permittee information used to manage authorized grazing and grazing related activity on public land; (2) maintain support documentation to manage authorizations; (3) maintain billing and collections information; (4) maintain grazing decisions; (5) maintain correspondence related to grazing authorizations and allotments; (6) document unauthorized use; (7) enable the BLM to effectively administer livestock grazing and associated activities on public lands; and (8) provide information to state, local and tribal governments, and other Federal agencies, businesses, organizations, and individuals to assist in transparency and promote the orderly administration of livestock grazing on public lands.

RAS provides data for the below listed reports which are available through the public-facing website Reports.BLM.gov.

- Allotment Information
- Allotment Master
- Authorization Use by Allotment

- Operator Information
- Permits Schedule

The reports available on the RAS website are generated from the information stored in the BLM rangeland administration electronic database. Allotment information provided includes allotment identification, size, amount of private, state, and public land administered; amount of forage use authorized, both active and suspended, for all operators using the allotment; proportion of forage in the allotment produced on public land; existence of an allotment management plan and identification of the grazing operator(s). Operator information provided includes authorization number, name, address, and date the authorization was issued, including expiration date; allotments used by operator; kind and number of livestock; and period of use and forage amount authorized for use by the operator.

In accordance with the BLM's INTERIOR/LLM-2, Rangeland Management System, 75 FR 82061 (December 29, 2010), individual and corporation names and addresses provided by grazing permittees will be included in reports available on the BLM accessible reports website. Telephone numbers, email addresses or financial information of individuals with a grazing authorization will not be made available on the publicly accessible reports website. INTERIOR/LLM-2 is currently being revised to provide updated content for the system and incorporate Federal government-wide requirements in accordance with OMB Circular A-108.

☐ No

Section 3. Attributes of System Data

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

Information is obtained directly from applicants during the application process and is presumed to be accurate at the time of submission. BLM Field Office staffs verifies accuracy of data extracted from application forms before it is entered into RAS. Other data will be verified through discussion with the customer.

B. How will data be checked for completeness?

BLM Field Office staff verifies accuracy of data extracted from application forms before it is entered into RAS. Other data will be verified through discussion with the customer.

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

Permits, leases, applications, bills, and correspondence are sent to the customers regularly and periodic telephone and face-to-face contacts are made with the customers. BLM Field Office

staff are responsible for entering assignations and data updates received from customers into RAS records in a timely manner.

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

RAS records are covered under the approved DRS/GRS/BLM Combined Records Schedules which is a combination of schedules developed by the National Archives and Records Administration (NARA), the Department of the Interior (DOI) and the Bureau of Land Management (BLM). The RAS record series description is Grazing Authorization Files, Master File; The Rangeland Administration System, and the records disposition authority is 4/14a(3)(a). The approved disposition authority for these records is permanent and cutoff instructions are every 5 years at the end of the fiscal year, in which BLM transfers a copy of the master file to NARA, along with the technical documentation, in accordance with 36 CFR 1235.44-50.

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

Permanent records are never destroyed and are always identified for transfer to NARA at a specific time after cutoff. Permanent records are transferred to the Federal Records Center (FRC) and then later transferred by the FRC to National Archives during NARA's annual move process. Permanent records may be transferred directly to the National Archives if they have met their disposition.

The RAS records are permanent and the disposition authority DAA-0049-2013-0004-0001 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." These disposition instructions can be found in the Combined Records Schedule under Schedule 4, Rangeland Administration System (RAS) Master File.

The procedures used to electronically transfer the records in RAS are in accordance with NARA Bulletin 2012-03, issued August 21, 2012. This Bulletin informed Federal agencies that, beginning October 1, 2012, NARA will use ERA for scheduling records and transferring permanent records to the National Archives. The procedures documented to electronically transfer data can be found in the Electronic Records Archive Agency User Manual.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction) affect individual privacy.

There is a moderate privacy risk due to the type and volume of personal information maintained in RAS. Information collected and used is limited to the minimum required to perform the

purpose and functions of RAS. To mitigate privacy risk, BLM has restricted access to personally identifiable information within RAS to a limited number of users.

Safeguards for RAS conform to the Office of Management and Budget (OMB) Circular A-130 and Department guidelines reflecting the implementation of the Computer Security Act of 1987 (40 U.S.C.759). RAS data is protected through user identification, strong passwords, database permissions and software controls. Such security measures establish different access levels for different types of users. For example, access rights for non-BLM users will allow them to query portions of the database but will not permit them to modify the data or to view personal information protected under the Privacy Act. Specific BLM employees will have a level of access that will allow them to enter new case information. Higher levels of access will allow authorized Bureau employees to grant or remove passwords, correct, or update the software, and impose of removing security controls.

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. RAS is classified as a moderate system for the Federal Information Security Modernization Act of 2014 and has all the required security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, RAS has controls in place to prevent the misuse of data by those having access to the data. Such security measures and controls consist of passwords, user identification, IP addresses, 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 RAS. All end-users have an individual password and ID that is issued by the RAS application steward. All new users will receive a user guide detailing the appropriate use of RAS. All DOI employees must complete mandatory privacy, security, records management, Controlled Unclassified Information, and Section 508 training, as well as role-based privacy and security training, annually, and acknowledge the DOI Rules of Behavior (ROB).

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 who have an official need 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 RAS logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing RAS 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 activity and user activity including invalid logon attempts and access to data via User Identification, Internet Protocol address, etc. Audit trails are also captured within RAS to determine who has added, deleted, or changed the data within RAS. Any qualification

overrides require that the account manager document the reasoning and the login name with date and time is added by RAS. The website uses https secure data transmissions.

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 consent received by the individual when providing information, by the publication of this PIA, the INTERIOR/LLM-2 SORN, the Privacy Act statement provided on the application forms, and the BLM RAS website (BLM Reporting Application - Rangeland Administration System Reports) provides a link to the DOI Privacy Policy page.

There is a risk that information may be maintained longer than necessary. This risk is mitigated by maintaining the records in accordance with the NARA-approved records schedules. The RAS grazing administrative support and management records strictly follow BLM Records Control Schedule 4/14a(3)(a). Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA Guidelines.

There is a risk due to the volume of the records designated as permanent and the processes involved in transferring to the National Archive. All permanent records are maintained in accordance with Bureau records policies and procedures which requires proper management of Federal records to ensure legality, integrity, access, and security standards are met. In addition, BLM monitors compliance to ensure proper and timely program practices including Permanent Records transfers to NARA, storage and retrieval operations, development and update of Records Schedules, management of litigation holds and freezes, and administration of internal program evaluations.

There is a risk that individuals submitting grazing applications may not have notice that BLM's public website (http://www.blm.gov/ras/) has a reporting capability, which makes reports available to the public from information stored in BLM RAS and which may contain a limited subset of PII. The reports include both allotment and operator information. Operator information provided includes the authorization number, name, address, date the authorization was issued, including expiration date. It also includes allotments used by the operator, kind and number of livestock, and period of use and forage amount authorized for use by the operator. The name, address, and authorization number are provided in consideration of a United States District Court, District of Idaho decision in Case No. CV 09-482-CWD. In that case, the Court found that there was substantial public interest in understanding the scope of the grazing and rangeland program, including knowing how many individuals or entities graze cattle on public lands, as well as the size and scope of their operations, and that this public interest outweighed the permit holders' privacy interest in their names, addresses and authorization numbers. This risk is mitigated by identifying court decision within the RAS PIA and the Supplementary Information section of the published SORN.

There is a risk of sharing information on the RAS public-facing website which produces a smaller subset of reports and makes them available externally to the public. The reports are

generated from the information maintained in RAS. This risk is mitigated by ensuring the BLM federal public website BLM Reporting Application - Rangeland Administration System Reports complies with existing laws and directives that address the need to protect the privacy of the American people when they interact with their government. Some of the key requirements for federal public websites that have been included for RAS are conducting a Privacy Impact Assessment and posting the DOI Privacy Policy link within the footer of the website which provides information on website security and additional required notices to members of the public who visit the any DOI website. In addition, System Owners and System Managers work closely with the BLM Privacy team to ensure external sharing of PII is only for authorized purposes and compatible with the purposes and routine uses described in the applicable SORN.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes:

The BLM uses forms to collect the relevant and necessary information required to authorize grazing on public lands (see 43 CFR Part 4130). Forms in the 4130 series are used by the public to apply for grazing use; apply for and/or transfer grazing preference; request exchange-of-use grazing agreements, and to report actual grazing use. The BLM has used these or similar forms to collect the necessary types of information for the last several decades for the purpose of approving or rejecting grazing applications, for tracking, collecting, and distributing grazing receipts, and to generate a variety of on-demand reports.

☐ 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

RAS does not create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly. BLM staff run reports on existing data such as counts of authorizations, counts of bills issued, total Animal Unit Months that are authorized on BLM lands, however this would not permit users to draw new conclusions or inferences about an individual.

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?

RAS does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☒ 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:

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

RAS provides data for reporting through the public-facing website Reports.BLM.gov that restricts the users to generating a variety of on-demand reports, including Allotment Information, Allotment Master, Authorized Use by Allotment, Operator Information, Permits Schedule Information, and Public Land Statistics. It is the responsibility of the information system owners to ensure no unauthorized data is disclosed.

All other data within RAS is limited to BLM users on a "need-to-know" basis for information that is required to perform an official function. Access is controlled by assignment of roles and

specific discrete authorizations and is limited to necessary access. System administrators may be afforded access to all of the data depending upon the system or application. It is the responsibility of information system owners to ensure no unauthorized access is granted.

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.

Contractors who work within BLM have access to the system if they are required to support an official business function or are involved with the development and maintenance of the RAS. The applicable security and privacy FAR clauses are included in the contracts.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

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

☒ Yes.

The Assessment and Authorization (A&A) process requires a system security plan (SSP) outlining the implementation of the technical controls associated with identification and authentication. The RAS SSP 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, IP Address, etc.

☐ No

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

The logs contain the user ID, date/time of access, invalid logon attempts, user activity, and as identified in the previous response, IP address for the employee who entered or modified the database record but does not link it to any other PII information.

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

RAS has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. In accordance with applicable DOI guidance, unauthorized activity will be included in the audit logs and alerts are being continuously updated to improve security. Logs are ingested by the BLM's Security Information and Event Management (SIEM) tool. The audit trail includes system user username, logon date and time, number of failed login attempts, and user actions or changes. The principle of least privilege is applied to ensure the system operates at privilege levels no higher than necessary to accomplish organizational missions or business functions. Authorized personnel may include security administrators, system administrators, system security officers, system programmers, and other privileged users. In addition, all users must complete annual Information Management Training, which includes, privacy, security, records management, and CUI, as well as role-based privacy and security training, prior to being granted access to the DOI network or any DOI system, and annually thereafter. All users are required to acknowledge and sign DOI ROBs which provides the guidance needed for users to fully understand the rules and their responsibilities. Also, embedded within the ROBs is the warning banner which is displayed upon logging into any Department of the Interior computer system. The warning banner clearly states all agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. It further states, by logging into an agency computer system, the user acknowledges and consents to monitoring of this system.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- ☒ Security Guards
- ☒ Key Guards
- ☒ Locked File Cabinets
- ☒ Secured Facility
- ☒ Closed Circuit Television
- ☐ Cipher Locks
- ☒ Identification Badges
- ☐ Safes
- ☐ Combination Locks
- ☒ Locked Offices
- ☐ Other.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *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 Assistant Director for WO-200, Resources and Planning, serves as the RAS Information System Owner and the official responsible for oversight and management of the RAS security controls and the protection of customer agency information processed and stored by RAS. 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 RAS. The Information System Owner is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the 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 Assistant Director for WO-200, Resources and Planning, 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 RAS Information System Owner, the Information System Security Officer and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the BLM Associate Privacy Officer.