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: Mineral and Land Records System (MLRS)

Bureau/Office: Bureau of Land Management (BLM)
Date: February 19, 2021
Point of Contact:
Name: Ashanti Murphy-Jones
Title: Acting BLM Associate Privacy Officer
Email: a1jones@blm.gov
Phone: 202-912-7012
Address: 20 M Street SE, Washington DC

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 Bureau of Land Management (BLM) has the responsibility for maintaining the land and mineral records for the United States. MLRS is a customer-centric, and geospatially enabled Land Information System that leverages data validation and standardized

business processes across the organization nationally and communicates land and case status changes across systems in real-time. Land status data includes land and mineral use authorizations (permits, O&G leases, Rights of Ways, mineral leases, etc), land title, (exchanges, acquisition, conveyances, etc.), and segregation (withdrawals, classifications) data extracted from the BLM's case files that support the BLM land, mineral and resources programs. MLRS consolidates legacy systems Legacy Rehost 2000 (LR2000), Alaska Land Information System (ALIS), and Oregon Land Status System (ORLSS) into a modernized land information management system. MLRS will handle such business processes as mining claims, oil and gas permitting, rights of way, and renewable energy leasing. It will provide BLM an integrated view across land status, case history, and current and historic information. It will also provide external customers the ability to securely perform land status research, submit and monitor applications, and maintain their profile and contact information via the Virtual Public Room. The Virtual Room uses Salesforce Customer Community. Esri-based geospatial capabilities embedded within the Virtual Public Room enable users to conduct geospatial research without leaving the Virtual Room.

Internal BLM users will use the MLRS User Console to perform the modernized LR2000, ALIS, and ORLSS case management functions, plus the additional functions required for the full MLRS solution (e.g., reporting through existing Oracle Business Intelligence Enterprise Edition (OBIEE) Enterprise Reporting, plus enhanced reporting, dashboards, and analytics through Salesforce Einstein Analytics). The User Console is powered by Salesforce Service Cloud and Salesforce Lightening Platform+ Unlimited Edition. Esri-based geospatial mapping capabilities are embedded in the MLRS User Console.

Another component of MLRS is the Enterprise Geospatial Management Services (EGMS) that will use the National Land Status Database (NLSDB) to provide spatial data to the MLRS Virtual Public Room and the MRLS User Console. The NLSDB will provide BLM a single source for real-time tabular and spatial data, including the Esri Enterprise Geodatabase and the Public Land Survey System. NLSDB data will be available for both internal BLM users and external public users. NLSDB will also be accessible directly by applicable BLM eGIS users, the eGIS system, and available to OBIEE for reporting purposes. EGMS and NLSDB will be hosted in the BLM NOC.

C. What is the legal authority?

Federal Land Policy and Management Act (43 U.S.C.1701)
The Uniform Relocation Act (42 U.S.C 4601)
The Act of April 25, 1812 (2 Stat 716)

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: 010-000002377; System Security and Privacy Plan for Mineral and Land Records 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.*
Case Recordation	Abstracted data from land and mineral, title, use authorization, and withdrawal cases	Yes	Names and addresses of customers
Mining Claims	Abstracted data from more than three million mining claim cases	Yes	Names and addresses of customers
Status	Contains historic data abstracted from title cases that transferred surface and/or mining rights to or from the U. S., and restriction of U.S. rights	Yes	Names and addresses of customers
Historic Index	Abstracted data from use authorization cases and withdrawal cases that were closed prior to the implementation of Case Recordation	No	n/a
PLSS	Contains land descriptions in accordance with the cadastral or special survey	No	n/a
Customer/Master Name	Contains, names, address, name entity identification numbers (NIDS) and the category of name entities.	Yes	Names and addresses of customers

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

☒ Yes:
This system is covered by the BLM - 32, Land & Minerals Authorization Tracking System, 56 FR 5014 (7 February 1991), modification published at 73 FR 17376 (April 1, 2008), which may be viewed at https://www.doi.gov/privacy/blm_notices. The BLM-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.

☐ No

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 30 June 2023

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: Case number, Interest relationships (the type of interest held), trespass, unauthorized access or use records and other information used to determine authorized use of lands. The system also contains percent and type of interest for Individuals, government entities, entrepreneurs, and other business entities holding permits, leases, or other authorizations to use public lands. Username and password is collected from individuals to access the MLRS system. Financial information of customers paying for requested data is collected through pay.gov, which may collect credit card payment information in addition to the above PII. Pay.gov is operated by the U.S. Department of Treasury and the Privacy Impact Assessment (PIA) for Pay.gov is at https://fiscal.treasury.gov/files/pia/paygov-pclia.pdf

B. **What is the source for the PII collected? Indicate all that apply.**

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☐ Other: *Describe*

D. What is the intended use of the PII collected?
Information in the system is collected for the purpose of establishing a record of transfers of title to and from the Federal Government and authorized uses of public lands. The MLRS system contains the names, addresses, interest relationships and percent interest for individual, government entities, entrepreneurs, and other business entities holding permits, leases, or other authorizations to use public lands. All trespass cases, unauthorized use cases, cultural resource cases, and paleontology cases are restricted from public viewing, and will be referred to BLM or Department of the Interior (DOI) law enforcement organizations and will be maintained in separate systems of records.

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

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

☒ Within the Bureau/Office:
The data in MLRS is used to determine land status. Land status is defined as the availability of a given tract of land for use (government or private) or the disposal or lease of the land (or its resources) into non-federal ownership or tenure. Status results from actions recorded in the cumulative set of documents and records that define

ownership and interest in lands and authorized uses on, and limitations to, use and ownership transfers. It is the BLM's responsibility to maintain the land and mineral data and it this data that is used to determine ownership and use of Federal lands and minerals. The agencies below have access to external data which does not contain PII.

☒ Other Bureaus/Offices:
The status of the land use may also be shared with other bureaus and offices as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking system of records notice. Additionally, trespass, unauthorized use, cultural resource, and paleontology cases may be shared with other DOI law enforcement organizations through the Incident Management, Analysis, and Reporting System (IMARS) for law enforcement investigations.

☒ Other Federal Agencies:
Information may also be shared with other Federal agencies as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking system of records notice.

☒ Tribal, State or Local Agencies:
Information may also be shared with tribal, state or local agencies as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking system of records notice.

☒ 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. Contractors do not have access to PII stored on the system.

☐ Other Third-Party Sources:

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

☒ Yes:

Individuals and corporations voluntarily provide information when applying to use, lease or permit on federally managed lands. The MLRS system contains the 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. If the information is not provided the application process cannot be completed.

☐ No:

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

☒ Privacy Act Statement:
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:
Notice is also provided through the publication of this privacy impact assessment and the BLM-32, Land and Minerals Authorization Tracking system of records notice, which may be viewed at https://www.doi.gov/privacy/blm_notices. Pay.gov and login.gov also provide privacy notice to individuals using their services. Individuals may view the pay.gov and login.gov privacy impact assessments for how their information is handled.

☒ Other:
When users access the system the following privacy act notice is displayed to the user:

System Use Notification

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. 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 verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the morning of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

☐ 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 data can be retrieved by individual name and case number.

I. Will reports be produced on individuals?

☒ Yes:
BLM employees can generate ad hoc and annual reports on land use when logged in to the internal system, which may contain names and addresses of individuals with interest in a case. For reports that are produced for external use, case types that contain sensitive data are flagged, and the sensitive data is suppressed from the data results.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?
BLM Field Office land mineral adjudication staff verifies the accuracy of data extracted from application forms prior to entry into MLRS System.

B. How will data be checked for completeness?
BLM Field Office land and mineral adjudication staff verifies completeness of data extracted from application forms prior to entry into MLRS System.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).
BLM Field Office land and mineral adjudication staff is responsible for entering designations and data updates from lessees/permittees into MLRS action records.

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 MLRS are covered by BLM records retention schedule 4/34 under disposition authority DAA-0049-2013-0004-0001, which was approved by the National Archives and Records Administration (NARA). The MLRS 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".

The retention period set forth by NARA on the MLRS system records are PERMANENT and covered by disposition authority DAA-0049-2013-0004-0001. Per the DRS/GRS/BLM Combined Records Schedule, the MLRS system is scheduled under

Schedule 4 item 34, LEGACY REHOST SYSTEM and Schedule 4/34(a), Master File. The content of the MLRS system and its modules includes land survey information and documentation of actions taken, abstracted from BLM case files, including case files information from ownership and authorization records, property rights and use permits affecting public lands, survey information, federal land and mineral ownership information, withdrawals, classifications and determinations, and bonding information. The database contains the 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.

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

The MLRS 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".

The disposition procedures set forth by NARA for MLRS are as follows; MLRS records are PERMANENT with cutoff every 5 years. 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". These disposition instructions can be found in the Combined Records Schedule under Schedule 4, Item 34(a), LEGACY REHOST SYSTEM (LR2000) Master File.

The procedures used to electronically transfer the records in MLRS 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 Electronic Records Archives (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.**

Safeguards for MLRS 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). All the MLRS 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, such as names and home addresses or private non- entrepreneurial individuals. 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 remove security controls.

There is a moderate privacy risk due to the type and volume of personal information maintained in MLRS. Information collected and used is limited to the minimum required to perform the purpose and functions of MLRS. To mitigate privacy risk, BLM has restricted access to personally identifiable information within MLRS to a limited number of users.

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. MLRS is a Moderate Impact system for FISMA and has all the required security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, MLRS 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 MLRS. All end-users have an individual password and ID that is issued by the MLRS application steward. All new users will receive a user guide detailing the appropriate use of MLRS. All DOI employees must complete mandatory privacy, security and records management training annually, and role-based privacy and security training, and sign 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 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 MLRS logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing MLRS must acknowledge the rules of behavior prior to each login. The System Security Plan describes the practice of audit trails. Audit trails are maintained per Department of Homeland Security (DHS), DOI

and BLM Security Policies. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by MLRS. 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 and the MLRS notice, and the Privacy Act statement provided on the application and the official BLM website. Individuals are also provided notice by the Department of Treasury when using pay.gov, and by the General Services Administration (GSA) when using login.gov. The PIA for pay.gov may be viewed at https://fiscal.treasury.gov/files/pia/paygov-pia.pdf. The PIA for login.gov may be viewed at https://www.gsa.gov/cdnstatic/20200911_-_logingov_PIA_signeddocx.pdf.

There is minimal risk due to the nature of the records being permanent. These records provide valuable insight into how public lands are managed by the US Government.

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:
MLRS provides Bureau employees and customers with a centralized source of land status information such as ownership (agency, State, etc.), use authorizations (permits, rights-of-way, mining claims, mineral leases, bond & surety, etc.), and segregation (withdrawals, classifications, etc.). Information in the system has been collected for the purpose of establishing a public 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:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

E. How will the new data be verified for relevance and accuracy?

No new data is derived.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.
  Consolidating data and processes in stages from Legacy Rehost 2000 (LR2K) and
  Alaska Land Information System (ALIS). The following controls will be in place
  to protect the data from unauthorized access or use: strong password requirements,
  session security, Trusted IP range, MFA, single-sign on, object and field level
  security, row-level access control, partitioning of data, sharing settings, encryption
  in transit and audit trail.

☒ Yes, processes are being consolidated.
  See above.

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

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

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

User access for MLRS is determined based upon the role of the BLM employee and
the level of access necessary to complete the user's functions. BLM users will access
MLRS using authentication through Security Assertion Markup Language (SAML)
and Active Directory.

MLRS provides authorized BLM users, access to create, read, update, and delete data,
and provide Serial Register Page reports on a case-by-case basis. The LR2000 Legacy
Reporting Data Base (LRDB) provides access for BLM users to all reports and access

for External users to various publicly available reports. The data in the LRDB is updated from the LTPDB on a nightly basis. MLRS Reports are web enabled. BLM DOI Office of Natural Resource Revenue, Bureau of Reclamation and U.S. Forest Service personnel access the MLRS Public reports via the internet. Public versions of the MLRS reports, minus sensitive and proprietary information, are accessible to the public via the Internet. The records shown on the BLM MLRS public site are all classified as Category 1 Records. It is the policy of the BLM to make records available to the public to the greatest extent possible, in keeping with the spirit of FOIA, while at the same time protecting sensitive information.

Public users will access the MLRS Virtual Public Room from any device with an internet connection by receiving authenticated access through login.gov, a service managed by GSA, integration with Salesforce. Authenticated external/public users include individual miners; company employees; consultants; and customer account managers. Unauthenticated public users (anyone not logged in; any citizen interested in information; other government agencies including Bureau of Reclamation, Department of Defense, Department of Energy, Federal Energy Regulatory Commission, National, Park Service, DOI Assistant Secretary of Land Mineral Management) may only research, perform visualizations of current land and mineral status, execute reports, and view fee schedules, run reports, and view real- time land usage data and potential conflicts.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?
Contractors who work at the BLM have access to the system. 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
MLRS uses the MuleSoft Anypoint Platform As a Service (PAAS) within the FedRAMP authorized MuleSoft Government Cloud to handle the critical interfaces between Salesforce and the BLM internal systems, like the Collection & Billing System (CBS) and Pay.gov. DocuSign SpringCM is a FedRAMP authorized Software As a Service that will be used by MLRS for creating, managing, and storing documents. It enables the creation of workflows that automate document generation with associated contractual terms, conditions, and stipulations for the legal forms required. This automation enables BLM to create an agreement from a library of approved templates and legal clauses, and automatically fill in customer information based on Salesforce fields. DocuSign SpringCM enables document redlining,

versioning, and activity tracking for every change made to an agreement. After adjudication, DocuSign SpringCM provides a repository that makes agreements searchable, even when the documents are only images of text.

☐ 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 MLRS SSP describes the practice of audit trails. Audit trails are maintained per Department of Homeland Security (DHS), Department of Interior (DOI) and Bureau of Land Management Security Policies.

☐ 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?

Violations of the following Rules of Behavior are considered IT security incidents. According to the Department of Interior Manual 375 DM 19.11B, all suspected actual or threatened incidents involving the destruction, physical abuse or loss of technological resources shall be reported to the appropriate authorities. BLM employees shall report observed security incidents to their supervisors or the local Information System Security Officer (ISSO). The ISSO may recommend the removal of any individual User ID and password from any BLM computer system in the event of a security incident. Other controls include access controls, least privileges, training, and monitoring user activities.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility

☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The BLM Assistant Director for WO-300, Energy, Minerals, and Realty Management, serves as the MLRS Information System Owner and the official responsible for oversight and management of the MLRS security controls and the protection of customer agency information processed and stored by MLRS. The Information System

Owner and the Privacy Act system manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in MLRS. 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 MLRS Information System Owner 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 MLRS 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.