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: Enhanced Abandoned Mine Land Inventory System (e-AMLIS)
Bureau/Office: Office of Surface Mining Reclamation and Enforcement (OSMRE)
Date: 07/14/2023
Point of Contact
Name: Patrick Dege
Title: Associate Privacy Officer
Email: osmre_privacy@osmre.gov
Phone: 202-208-3549
Address: 1849 C Street NW, 1200W, Washington, DC 20240

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 Surface Mining Control and Reclamation Act (SMCRA) was amended in 1990 to add Section 403(c) which required the Secretary of Interior to maintain an inventory of high priority coal sites and provide standardized procedures for States and Tribes to use in updating the

Inventory. The 1990 amendment also required that the Inventory be updated on a regular basis, not less than annually, and authorized funding and technical assistance to the States and Tribes for this purpose. The 1990 amendment and the need for an automated nationwide Inventory led to the creation of earlier versions of the Enhanced Abandoned Mine Land Inventory System (e-AMLIS) as a compilation of the individual State, Tribe, Federal Reclamation Program (FRP), and Rural Abandoned Mine Program (RAMP) inventories of abandoned mine land (AML) problems.

The e-AMLIS system is a relational database that documents unfunded high priority coal reclamation projects and records when funding is made available for each problem area. Reports from e-AMLIS include completed coal projects which play a central role in making the determination that a State or Tribe has addressed all known coal problems and records the accomplishments of Certified States and Tribes completing non-coal and other activities. Further, e-AMLIS is a source of information on the amount of work completed under a State/Tribal program, and the extent and estimated cost of AML problems remaining to be abated.

The e-AMLIS system is used to store, manage, and report on the OSMRE inventory of AML problems. This includes lands in need of reclamation and issues concerning lands that have been reclaimed. The inventory contains information on the location, type, and extent of AML impacts, as well as information on the cost associated with the reclamation of those problems. The inventory is based upon field surveys by State, Tribal, and OSMRE program officials. It is dynamic to the extent that it is modified as new problems are identified and existing problems are reclaimed.

e-AMLIS incorporates AML point locations generated by GIS (Geospatial Information System) software when States and Tribes enter location coordinates either by decimal degrees or degree minutes and seconds.

The e-AMLIS Key is the primary identifier for the Problem Area (PA) and is depicted by a combination of a State or Tribe's abbreviation and the PA_NUMBER. Data fields associated with the e-AMLIS key include the: name of the problem area; dates prepared and revised; field contact information; preparer contact information; planning unit name and number; Latitude and Longitude; Congressional district; watershed; quadrangle; county; Federal Information Processing Standard (FIPS) code; Hydrologic Unit Code (HUC); mining type; percentage of surface owners; ore types; problem types; program; alternate funding sources; imperial units; metric units; costs; Government Performance Results Act (GPRA) acres; supporting documentation uploaded in various formats for each problem type; comments fields for problem types and problem areas; completion date; project name; number of people no longer at risk (census); people no longer at risk (estimated); miles of streams reclaimed; number of impounded acres; and completion comments.

e-AMLIS access is tiered based on user credentials. The general public or any interested party can log into the e-AMLIS system as a guest, but guests cannot modify data and some information may not be viewable. OSMRE, State, and Tribal level users are given elevated

privileges that allow them to modify data but there are controls such as they can only create and modify information within their assigned jurisdictional area. The OSMRE e-AMLIS administrators are given the highest level of access to modify data in order to assist customers with access issues and create accounts for credentialed users.

C. What is the legal authority?

- The Surface Mining Control and Reclamation Act of 1977 (30 U.S.C. §§ 1201–1328)
- The Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521) requires federal agencies to minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information.
- Government Organization and Employees, Departmental Regulations (5 U.S.C. 301)
- Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)
- E-Government Act of 2002 (Public Law 107-347)
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

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 DOI's Governance, Risk, and Compliance platform?

☒ Yes: *Enter the UII Code and the System Security and Privacy Plan (SSPP) Name*

UII Code: 010-000000722. The SSPP is currently in development.

☐ 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.*
None	None	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)*

☒ No

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

☒ Yes: *Describe:*

OMB Control #:1029-0087, The AML Problem Area Description Form OSM-76; Expiration Date: 7/31/2025

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: *Specify the PII collected:*

The e-AMLIS OSM-76, The AML Problem Area Description Form displays the name and work phone number of the OSMRE, State, or Tribal staff who prepared the form for the AML site within their jurisdiction and/or the field contact. The OSM-76 form contains information on individual AML sites to include their size and location along with the problems inherent to the site. Additionally, an estimate of funding required to mitigate the issue, or the funding allocated.

For OSMRE, State, and Tribal credentialed users, name, organization affiliation, work address, work email address, and work phone number are required to create user accounts, which are provided by the users in the e-AMLIS Account Request Form. The system also contains the individual's username and password which are required to access data in the system. Although employees may provide a personal email address and phone number it is not recommended and is highly discouraged.

When seeking online system support, individuals may provide their name, phone number, and email address to resolve any issues or address questions.

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 ('fill-able' PDF, transmitted digitally via email)
☒ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems: *Describe*
☐ Other: *Describe*

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

The PII collected is to record State/Tribal AML reclamation efforts. State/Tribal staff are responsible for tracking the units and costs of reclamation construction projects in their jurisdictions. These projects are entered into e-AMLIS and tagged with the individual's name and work phone number. The e-AMLIS system also auto-generates email communications using the individual's work email address.

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.*

An OSMRE e-AMLIS Administrator can create or maintain user accounts. OSMRE e-AMLIS staff may modify or export view data from the system within their area of jurisdiction to be used to complete routine services for customers, report metrics, and conduct data quality reviews.

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

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

Information may be shared with law enforcement organizations as necessary for any investigations related to a violation or entity involved in an investigation.

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

State and Tribal e-AMLIS staff can view and alter information within their area of jurisdiction and may export data from the system to be used to complete routine services for customers, report metrics, and conduct data quality reviews.

The e-AMLIS system records the name and work phone number of the OSMRE and/or the State/Tribal partner entering and editing the data within the system on the OSM-76 form.

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

e-AMLIS hosting contractor staff have access to the backend of the e-AMLIS system and can run queries, export data, and modify data through the backend if needed as well as to provide continuous monitoring, vulnerability management, contingency planning, Federal Information Security Modernization Act (FISMA) compliance, intrusion detection, and incident response.

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

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.*

The e-AMLIS system records the users' name and work phone number to track reclamation project lifecycle and historical information. e-AMLIS also uses the users' work email to transmit auto-generated system notices (emails) and updates. Should the user decline to submit this information, they are not eligible to work in the e-AMLIS System.

☐ 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.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment (PIA). A privacy notice will be added to the e-AMLIS Account Request Form, and e-AMLIS Contact Support webpage.

☒ Other: *Describe each applicable format.*

Users are presented with a System Use Notification banner on the e-AMLIS website that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ 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 system retrieves data using the e-AMLIS key which is the primary identifier for the Problem Area (PA) and is depicted by a combination of a State or Tribe's abbreviation and the PA_NUMBER. OSM-76 Problem Area Descriptions (PADs) record the user's name and work phone number as they track their jurisdiction's AML projects through their lifecycle. The e-AMLIS system also utilizes users' work email addresses to send auto-generated messages regarding PAD statuses.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

User account data is collected on the e-AMLIS Account Request Form to obtain an e-AMLIS user account. If there is an issue with the information provided on the account request form, the OSMRE e-AMLIS Administrator or Coordinator will contact the applicant for updated or corrected information.

Whenever data quality reviews or other routine tasks indicate a record may not be accurate in the e-AMLIS user account, or via individual state and tribes, the OSMRE e-AMLIS Coordinator follows up with the appropriate contact to attempt to resolve the issue.

B. How will data be checked for completeness?

User account data is collected on the e-AMLIS Account Request form to obtain an e-AMLIS user account. If there is an issue with the information provided on the account request form, the OSMRE e-AMLIS Administrator or Coordinator will contact the applicant for updated or corrected information.

Whenever data quality reviews or other routine tasks indicate a record may not be complete or accurate in the e-AMLIS user account, or via individual state and tribes, the OSMRE e-AMLIS Coordinator follows up with the appropriate contact to attempt to resolve the issue.

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

Entities or users applying for e-AMLIS access or entering AML information are responsible for ensuring data is current. However, if/when discrepancies or errors are brought to the attention of the e-AMLIS Coordinator, the record(s) are corrected manually by an e-AMLIS Administrator or returned to the State/Tribal user for correction.

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

e-AMLIS records are maintained under OSMRE Records Schedule N1-471-10-005, Enhanced Abandoned Mine Land Inventory System (e-AMLIS), which was approved by the National Archives and Records Administration (NARA).

Master Data Files have a disposition of PERMANENT. Copies of the master data files are to be transferred to the National Archives at end of every 3rd calendar year to the National Archives as specified m NARA standards at time of transfer.

Reference Data Files have a disposition of TEMPORARY. Destroy or delete when no longer needed for business use or reference need.

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

Approved disposition methods include shredding, burning, or pulping paper records, and degaussing or erasing electronic records in accordance with NARA guidelines and Departmental policy. However, data (electronic and paper) files transferred to the Federal Record Center (FRC) are disposed of via methods determined by the FRC.

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 privacy risk to individuals that is mitigated by the security and privacy controls implemented to safeguard privacy and the limited collection of personally identifiable information (PII) from individuals. For credentialed users PII maintained in the system is constrained to name, username, password, organization affiliation, and work email address and work phone number that are required to create and manage user accounts. The protection and maintenance of information for recovery and backup purposes is done following OSMRE policy and process for backup and retention of information. System permissions and access controls are in place to limit system access to only those authorized individuals with the proper authorization to perform official functions.

There is nominal risk to the privacy of official user information throughout the information lifecycle. Risk is reduced by following established guidance from the National Institute of Standards and Technology (NIST) Special Publication SP 800-53 on access controls. Privacy risk to e-AMLIS system accounts would affect usernames and passwords. The e-AMLIS system is hosted in a certified FedRAMP cloud-based environment and has a Moderate system security categorization in accordance with NIST standards., FIPS 199, and the FISMA, and FISMA compliance.

There are privacy risks related to hosting, processing, and sharing of data. These risks are mitigated through a combination of physical, administrative, and technical controls. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. The e-AMLIS system utilizes appropriate security and privacy controls implemented to safeguard information collection, use, retention, processing, disclosure, destruction, transmittal, storage, and audit logging. It covers access controls, password management, firewalls, segregation of duties, and encryption of database, media, and communications. The e-AMLIS system utilizes the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following NIST, FISMA, OSMRE, and DOI security and privacy policies. All access is controlled by authentication methods including multi- factor authentication (MFA). All DOI employees and contractors are required to complete initial and annual security and privacy awareness training and sign DOI Rules of Behavior. Additionally, all State and Tribal employees and contractors are required to complete to sign the "*State and Tribal Users Rules of Behavior for the Enhanced Abandoned Mine Land Inventory System (e-AMLIS)*". OSMRE Personnel authorized to manage, use, or operate the e-AMLIS System application are required to take additional role-based privacy and security training annually. e-AMLIS System data is under the control of its system owner, the OSMRE Headquarters Program Assistance Division, Reclamation Support Chief, who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use, and for meeting privacy requirements, including providing adequate notice, making decisions on requests for notification, access, and amendments, as well as processing complaints, in consultation with OSMRE and DOI privacy officials. Information may be shared with law enforcement organizations as necessary for any investigations related to a violation or entity involved in an investigation. However, appropriate safeguards such as encrypted media is utilized to ensure that PII is protected.

There is a risk of unauthorized access, use or disclosure of the records in the system. There is also a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. These risks are mitigated by safeguards including access restrictions based on least privilege, use of username and password, role-based training, and other controls to ensure the confidentiality, integrity, and availability of the records. The authorized personnel and system administrators' complete privacy, security, records, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information awareness training and privacy and security role-based training initially and on an annual basis. Access to records in the system is limited to authorized personnel whose official duties require such access. The system uses audit logs to protect against unauthorized access, changes, or use of data. Electronic data will be protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual's web browser is encrypted using approved federal encryption protocols that meet NIST standards. These security measures will establish different degrees of access for different types of users. Ongoing system development will require MFA, at the point of entry as another security control to mitigate the risk of unauthorized access, use or disclosure of the records in the system. The e-AMLIS contract provides continuous monitoring, vulnerability management, contingency planning, FISMA compliance, intrusion detection, incident response, and assessment and authorization (A&A).

There is a risk that users may not receive adequate notice of the purpose and uses of their information. This risk is mitigated by notice posted on the OSMRE e-AMLIS Account Request Form, e-AMLIS site including the Contact Support webpage, a System Use Notification, and this PIA. Username and work email address is collected directly from the individual and is used for the purpose of creating user accounts, authenticating users to the site, and granting access to the data contained within the e-AMLIS system.

There is a risk that records may be maintained longer than authorized or necessary to meet a business need. Records are maintained in accordance with a NARA approved schedule. Once the retention period is deemed to be over, the records are destroyed in accordance with approved methods as outlined in DOI policy and the applicable records schedule.

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:

SMCRA requires OSMRE to maintain an inventory of high priority coal sites and provide standardized procedures for States and Tribes to use in updating the Inventory. e-AMLIS provides State/Tribal partners the means to enter the required data and edit the data appropriately. Their name and work phone number are tagged to each PAD (OSM-76 form) they add/edit within the system.

☐ 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?

N/A - The system does not derive new data or create previously unavailable data.

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:

Regional/Field Office staff from OSMRE will see the State/Tribal users' names and work phone numbers on each PAD (OSM-76 form).

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

Anyone who consents to the System Use Notification can access the publicly accessible information as a guest user but has no ability to edit, modify, or change data. They also cannot view all information stored in the database, for example site location data is generalized (truncated) so that specific location information is not viewable to non-credentialed guest users. Additionally, public users cannot access supporting documentation uploaded within the system.

Users with credentials receive elevated permissions to e-AMLIS which corresponds to their work duties. e-AMLIS users are given a role based on their work affiliation (state/Tribal or OSMRE). Their access to user information is limited to users' name and work phone number and they do not have privileges to create or modify records for other states or tribes outside of their assigned jurisdiction. OSMRE e-AMLIS administrators are granted access to modify any data in the system in any jurisdiction and create and manage user accounts.

A limited number of OSMRE information management staff and the e-AMLIS hosting contractor staff have access to the backend of the e-AMLIS system and can run queries, export data, and modify data through the backend if needed.

Electronic data is protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual's web browser is encrypted using approved federal encryption protocols. These security measures establish different degrees of access for different types of users.

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?*

The appropriate Privacy Act contract clauses were included in the contract. Current contracts not in compliance with the Information Technology (IT) Baseline Compliance Contract Guidelines memorandum of August 15, 2022, will be modified to include the appropriate privacy terms and conditions.

☐ 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.

e-AMLIS users' actions and activities are recorded on each PAD (OSM-76 form) and the PAD's History. The purpose of e-AMLIS is not to monitor individuals, however user actions and use of the system are logged in compliance with DOI security policies. Data captured include username, user's last date of login, date of user content creation, and date user content was modified. Additionally, the application tracks the IP that accessed the system, user's login/logout and how long they are in the system.

When a registered user performs a system function, a record of that activity is created and is attributed to them. The system does not actively monitor portal users and is not programmed to do so.

☐ No

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

The system does not actively monitor portal users and is not programmed to do so. Audit logs are maintained in the system and track login attempts and errors. Audit logs record username, date/time, and actions. Account activated, account updated, password changes, account activity (on PADs), and account deleted are all examples of account auditing of the system tracks.

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

The applications governance plan outlines the roles and responsibilities of users with elevated access to the administration functions. The outline uses the principle of least privilege to provide only the level of access required to perform in their role. Audit logs capture user actions and use of the system, which are monitored to meet OSMRE and DOI security policies.

The e-AMLIS contract provides continuous monitoring, vulnerability management, contingency planning, FISMA compliance, intrusion detection, and incident response.

Only authorized system administrators can access system auditing information.

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*

MFA is required from credentialed users and must be U.S. based to access the application.

(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*

Annual role-based security and privacy training is required for OSMRE credentialed users and administrators.

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 OSMRE Headquarters, Program Assistance Division, Reclamation Support Chief, serves as the OSMRE e-AMLIS System Owner and the official responsible for oversight and management of the OSMRE e-AMLIS system security controls and the protection of agency information processed and stored by the OSMRE e-AMLIS system. The Reclamation Support Chief and Information System Security Officer (ISSO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies, as well as processing complaints, in consultation with the OSMRE Associate Privacy Officer (APO).

The OSMRE e-AMLIS System Owner is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting privacy requirements including the reporting the loss, compromise, unauthorized disclosure, or access of individuals' personal information, in consultation with the OSMRE APO.

The OSMRE Incident Response Team handles incidents in accordance with OSMRE incident response policy and the DOI Privacy Breach Response Plan, which provides guidance on breach response, the process for timely notification to individuals, and other remedial actions.

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 OSMRE e-AMLIS System Owner is responsible for oversight and management of the OSMRE e-AMLIS system security and privacy controls, and for ensuring to the greatest possible extent that the OSMRE e-AMLIS system is properly managed, and that access is granted in a secure and auditable manner.

The OSMRE e-AMLIS System Owner and ISSO are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the OSMRE APO and the OSMRE Incident Response Team in accordance with the DOI Privacy Breach Response Plan and the OSMRE Incident Response Plan.

e-AMLIS system administrators and users are required to report any potential loss or compromise to the OSMRE e-AMLIS System Owner, ISSO and the OSMRE APO.