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: Minerals Revenue Management Support System (MRMSS)
Bureau/Office: ONRR Information Management Center
Date: 8/05/2019
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: 202-208-1605
Address: 1849 C Street NW, Room 7112, 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 Minerals Revenue Management Support System (MRMSS) is a major application that is managed by the Department of the Interior (DOI) Office of Natural Resources Revenue (ONRR) to process bonuses, rents, and royalties received from mineral leases on Indian lands. The primary purposes of the system are to collect royalties and rents; control revenues; distribute funds collected; maintain records of royalty accounts and associated sales and production information; provide data to facilitate comparative auditing of mineral production, royalties due, revenues collected, and funds distributed;

gather statistics for managing the mineral leasing program; provide informational access to external users including states, Indian tribes or agencies, and Federal agencies; and provide outreach services to the Indian community.

ONRR is responsible for the management of all revenue associated with both Federal offshore and onshore mineral leases. ONRR, in conjunction with the Bureau of Indian Affairs (BIA), provides revenue management services for mineral leases on Indian lands. ONRR uses the MRMSS to process the bonuses, rents, and royalties received from leased lands and provides the Federal Government with one of the largest sources of non-tax revenue.

MRMSS consists of three subsystems, MRMSS Financial Subsystem (FS), MRMSS Data Warehouse (DW), and MRMSS Compliance. This privacy impact assessment addresses the privacy risks for MRMSS and the subsystems.

- The FS subsystem is used for accounting for and distributing money that the Government collects from energy companies for both conventional energy and renewable energy on Federal and Indian lands. FS is MRMSS' transactional database and falls under the Chief Financial Officers Act of 1990. FS is comprised of a commercial off-the-shelf (COTS) software application that has been configured and customized for ONRR's business processes. The primary processes include royalty reporting, rent and bonus reporting, royalty payments, distribution and disbursements. In addition, a web application has been developed to collect and deliver regulatory reporting data from individual reporter sources. The reporting includes royalty, production, rental, and electronic payments for rentals (Federal only). This also includes the ability to perform reporting, retrieval, uploading, downloading and edit validation.

- The DW/Business Automation Services subsystem is comprised of COTS software applications and several web applications developed to provide DW/Business Automation Services, as well as business intelligence tools, maintaining historical and current information associated with the management of all revenues, including royalty, production, accounts receivable, and distribution information.

- The Compliance subsystem is used to ensure companies comply with laws, regulations and lease terms and pay correctly. This subsystem is composed of several web applications developed to provide Tracking, Compliance, Reporting and Verification Tools used to support compliance activities.

C. What is the legal authority?

The Federal Oil and Gas Royalty Management Act of 1982, 30 U.S.C. 1701–1759; 25 U.S.C. Chapter 12, addressing the lease, sale, or surrender of allotted or unallotted lands found at 25 U.S.C. 391–416j; 30 U.S.C. Chapter 3A, addressing leases and prospecting permits, found at 30 U.S.C. 181–196; and the Outer Continental Shelf Lands Act, 43 U.S.C. 1331–1356b.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

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

010-000000710; System Security Plan (SSP) for Minerals Revenue Management Support 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.*
Compliance Subsystem (CS)	Compliance, Tracking, Reporting and Verification of Royalty reporting and distribution	Yes	The Office Workload Management System (OWMS) a .NET application automates the management Allottee inquiries pertaining to payments as well as generate management reports related to outreach meetings and customer service - Lease numbers related to Individual Indian Mineral Owners/Accounts, address and phone numbers

Financial Subsystem (FS)	Accounting and distribution of royalties collected by the Federal Government	No	N/A
Data Warehouse (DW)	Business Automation, business intelligence and data warehouse reporting	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)*

OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016, which may be viewed on the DOI Office of the Secretary SORN website at https://www.doi.gov/privacy/os-notices.

☐ No

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

☒ Yes: *Describe*

- 1012-0001: Accounts Receivable Confirmations, expires February 28, 2022
- 1012-0002: 30 CFR parts 1202, 1206, and 1207, Indian Oil and Gas Valuation, expires February 28, 2022
  - Form ONRR-4109, Gas Processing Allowance Summary Report
  - Form ONRR-4110, Oil Transportation Allowance Report
  - Form ONRR-4295, Gas Transportation Allowance Report
  - Form ONRR-4410, Accounting for Comparison (Dual Accounting)
  - Form ONRR-4411, Safety Net Report
- 1012-0003: 30 CFR parts 1227, 1228, and 1229, Delegated and Cooperative Activities with States and Indian Tribes, expires December 31, 2021
- 1012-0004: 30 CFR parts 1210 and 1212, Royalty and Production Reporting, expires March 31, 2022
  - Form ONRR-2014, Report of Sales and Royalty Remittance
  - Form ONRR-4054-A,B,C, Oil and Gas Operations Report
  - Form ONRR-4058, Production Allocation Schedule Report
- 1012-0005: 30 CFR parts 1202, 1204, and 1206, Federal Oil and Gas Valuation, expires March 31, 2020
  - Form ONRR-4393, Request to Exceed Regulatory Allowance Limitation

- 1012-0006: 30 CFR part 1243, Suspensions Pending Appeal and Bonding, expires February 28, 2021
  - Form ONRR-4435, Administrative Appeal Bond
  - Form ONRR-4436, Letter of Credit
  - Form ONRR-4437, Assignment of Certificate of Deposit
- 1012-0008: 30 CFR part 1218, Collection of Monies Due the Federal Government Expires April 30, 2021
  - Form ONRR-4425, Designation Form for Royalty Payment Responsibility
- 1012-0009: 30 CFR part 1220, OCS Net Profit Share Payment Reporting, expires December 31, 2020
- 1012-0010: 30 CFR parts 1202, 1206, 1210, 1212, 1217, and 1218, Solid Minerals and Geothermal Collections, expires January 31, 2020
  - Form ONRR-4430, Solid Minerals Production and Royalty Report
  - Form ONRR-4292, Coal Washing Allowance Report
  - Form ONRR-4293, Coal Transportation Allowance Report
  - Form ONRR-4440, Solid Minerals Sales Summary

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Financial Information
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Individual owner identification, allocated ownership percentage, and estimated revenues from leases. PII is used to support the Indian Outreach Program for Individual Indian Mineral Owners as part of royalty-related problem resolution for those owners. Contact information is voluntarily provided to ONRR and included in MRMSS for the purpose of following up regarding royalty-related issues of interest to the individuals and for the benefit of the individuals.

The system also contains records concerning corporations and other business entities that are not subject to the Privacy Act, as well as data on a small proportion of sole proprietors, which is covered by the Privacy Act. Records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information. PII collected from sole proprietors includes fax numbers, email addresses, other contact information, customer identification number, lessee and/or payor information, Tax Identification Number, collection actions, bank account number, check

number, amount paid, contract number, and other information related to types of lease, sales and revenues that may be generated or maintained during the processing and administration of minerals revenue management responsibilities.

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 *Describe*
☒ Other: *Describe*

Authorized ONRR users have access to the Trust Asset and Accounting Management System (TAAMS), the system of record for title and land resource management of Indian Trust and Restricted Land within DOI and BIA, to manually retrieve data regarding lease ownership of the Individual Indian Mineral Interest Owner (IIMIO). The information is transferred manually and kept in a paper file, and no information is put into electronic form into the OWMS portion of MRMSS, except for a name and a case number, which is used for the paper filing system kept locked in ONRR offices.

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

PII is used to verify royalty payments to Tribes and Individual Indian Mineral Interest owners. Subjects have an option to call ONRR State and Indian Outreach (SIO) and provide their PII data in order to provide contact information which is kept in a paper file. During outreach events, subjects provide their PII data to SIO employees.

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.*

PII is shared within ONRR for the collection, disbursement and verification of revenues from energy production that occurs onshore on Federal and American Indian lands. This information assists ONRR in the verification of royalties paid to Individual Indian Mineral Interest Owners.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
PII is shared with other DOI bureaus, including BIA, Bureau of Land Management, and the Office of the Special Trustee, to facilitate comparative auditing of mineral production, royalties due, revenues collected, and funds distributed; gather statistics for managing the mineral leasing program; provide informational access to external users including states, Indian tribes or agencies, and Federal agencies; and provide outreach services to the Indian community.

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

PII may be disclosed with other Federal agencies for the purpose of submitting reports, data and information related to the production of minerals such as oil, gas and solids associated with the management of revenues. Other disclosures may be made to external agencies as outlined in the routine uses in OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

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

Information may be shared with Tribal, State or local agencies when authorized or required by law, as outlined in the as outlined in the routine uses in OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

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

Information may be shared with a DOI contractor (including employees of the contractor) that performs services requiring access to these records on DOI's behalf to carry out the purposes of the MRMSS system as necessary and authorized, or if it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised and sharing information is necessary to remediate the compromise.

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

Disclosures may be made to third parties when authorized and necessary to perform official functions of ONRR, as outlined in the routine uses in OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Information is voluntarily provided to ONRR for the purpose of following up regarding royalty-related issues of interest to the individuals and for the benefit of the individuals.to process bonuses, rents, and royalties received from mineral leases on Indian land, and to support the Indian Outreach Program for Individual Indian Mineral Owners as part of royalty-related problem resolution for those owners and provide outreach services to the Indian community. SIO validates the identity of individuals through oral discussion and enrollment number for further information related to royalties or mineral related questions. Individuals can decline to provide PII data. Customer service requests are initiated by individuals, and PII data is needed to access data to provided customer service. If the information is not provided, ONRR employees cannot contact the individual with the results of the service or inquiry requested by the individual.

☐ 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.*

This information is requested under 30 U.S.C. 1701–1759, 25 U.S.C. 391–416j; 30 U.S.C. 181–196; and 43 U.S.C. 1331–1356b for the purpose of facilitating mineral lease revenue management. This information will be used to process bonuses, rents, and royalties received from mineral leases on Indian lands. Information may be disclosed to the Office of Natural Resources and Revenue officials to ensure compliance with Federal and agency mineral lease revenue requirements. Information may also be disclosed to other Federal agencies for the purpose of submitting reports, data and information related to the production of minerals such as oil, gas and solids associated with the management of revenues, and other routine uses identified in the OS-30, Minerals Revenue Management Support System (MRMSS) system of records notice, which may be viewed at https://www.doi.gov/privacy/sorn. Providing the information is voluntary; however, not providing the requested information may delay processing of bonuses, rents, and royalties received from mineral leases on Indian lands.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this PIA and the OS-30, Minerals Revenue Management Support System (MRMSS) SORN, 81 FR 16207, March 25, 2016.

☐ Other: *Describe each applicable format.*

☐ None

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

Customer records may be manually retrieved by name or customer identification number, owner name, or owner identification number, lease or contract number, lessee and/or payor, permittee, production reporter, or commodity.

I. Will reports be produced on individuals?

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

Reports are generated to provide royalty and production information related to IIMIO leases. Reports are viewed on screen and only printed when extenuating circumstances required further analysis. The printed report is kept in a paper file. ONRR employees supporting IIMIO have access to the paper files and they are only shared with the specific IIMIO.

☐ No

Section 3. Attributes of System Data

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

The PII data for IIMIOs is collected from them directly so is assumed to be correct at the time of collection, and is not further verified for accuracy.

B. How will data be checked for completeness?

The PII data for IIMIO is collected from them directly so is assumed to be correct at the time of collection, and is not further verified for completeness.

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

Information collected from individuals is checked as part of the initial contact.

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

Records in this system are maintained under the Minerals Management Service (MMS) Comprehensive Schedule approved by NARA (NC1-057-84-07), which include both permanent and temporary dispositions. These records are subject to litigation holds and permanent retention. Administrative records and general correspondence files have temporary dispositions and are maintained in accordance their respective records schedules dependent on the specific subject matter or function and retention requirements. Temporary mission files related to mineral resource, lease and royalty management activities are cut off at the close of the fiscal year then transferred to the Federal Records Center, one year after cutoff, and eligible to be destroyed 7 years after cutoff, providing no records holds or litigation holds are in effect.

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 384 Department Manual 1 and NARA guidelines.

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 risk to individual privacy resulting from:

1. Physical or technical breach of the system by internal or external threats which result in the exposure of information;
2. Access to information without proper authorization from external users of the system;
3. Terminated user access is not completed in a timely fashion; or
4. Role and access assignments may be made in error.

These risks are mitigated by the controls implemented to safeguard PII and network security in accordance with the overall moderate security categorization pursuant to the Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. MRMSS is compliant with the Privacy Act of 1974, Federal Information Security Modernization Act (FISMA), Joint Financial Management Improvement Program (JFMIP)/Federal Accounting Standards Advisory Board (FASAB), Office of Management and Budget (OMB) Circulars A-127 and A-130, and National Institute of Standards and Technology (NIST) standards. Privacy risks are mitigated through the design and implementation of appropriate privacy and security controls throughout the information system based on the NIST Special Publication 800-53, Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations, and implemented controls are regularly assessed for effectiveness and assurance. Computer servers in which electronic records are stored are located in secured DOI and contractor facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI

network and information assets.

The MRMSS incorporates configuration management to ensure that technology flaws and vulnerabilities are identified and remediated, that information technology resources are configured for least privilege and separation of duties, and follow least functionality practices. These secure configurations are applied for the databases, operating systems, applications, and networking rules employed for the MRMSS.

The MRMSS is designed to ensure secure communications protection controls are implemented to protect data confidentiality, integrity and availability through the use of encryption and secure communications design, which include defense in depth measures such as, firewalls, routers, intrusion protection and detection, and the usage of secure protocols for the transmission of information. Information integrity controls ensure that data and information input into the MRMSS is checked and validated for proper formats and expected values, and prevent the execution of malicious code from users of the system. Additional data protection controls ensure electronic data is protected through user identification, passwords, database permissions and software controls.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. Access control to the MRMSS employs both manual and technical controls to ensure that users of the system are authorized to access the system, their access to system resources is managed and implements need to know, least privilege, and separation of duties while using the system, and are properly authenticated to use the system with multiple factors of authentication. Users of the system are reviewed on a periodic basis, and user access is adjusted regularly for users who no longer have a need to use the system, are no longer employed, users who undergo role changes and no longer need access to perform their job. Access control also ranges from disabling after periods of inactivity to account termination when there is no longer need for access to the system.

Audit logging is implemented to capture user information as well as security configuration information for the MRMSS. This logging activity allows administrators and information technology security personnel to identify changes to access or configuration of the system, and provides an audit trail record for research into incidents and events that may occur. This logging is configured to include types of events, dates and times of events, user identification, as well as the success and failure of events.

The MRMSS undergoes Authorization and Accreditation activities on an ongoing basis through the implementation of continuous monitoring, and undergoes annual audits, as well as several ad hoc control assessments throughout the calendar year. These assessment activities test the effectiveness and functionality of the controls implemented, and result in assurance that the controls in place are working as intended. At times these assessments result in findings that become corrective actions to improve the effectiveness, functionality and operation of the security controls implemented. This assessment and continuous monitoring activity ensures compliance with NIST special publications as well as OMB policy. All users of the MRMSS undergo awareness training

and are required to follow established internal security protocols, and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The purposes of the system are to collect royalties and rents; control revenues; distribute funds collected; maintain records of royalty accounts and associated sales and production information; provide data to facilitate comparative auditing of mineral production, royalties due, revenues collected, and funds distributed; gather statistics for managing the mineral leasing program; provide informational access to external users including states, Indian tribes or agencies, and Federal agencies; and provide outreach services to the Indian community.

☐ 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?

Not applicable. MRMSS 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. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

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

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

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

User access is managed by "need-to-know" through role-based access controls, implementing least privilege and separation of duties concepts so that each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. Access to information to perform official functions is restricted through technical, logical and administrative controls, to include vetting, periodic review and termination when "need-to-know" is no longer valid.

User access to system resources is managed and implemented on least privilege and separation of duties principles, and uses are properly authenticated with multiple factor authentication. Users of the system are reviewed on a periodic basis, and user access is adjusted regularly for users who no longer have a need to use the system, are no longer employed, users who undergo role changes and no longer need access to perform their job. Access controls also range from disabling after periods of inactivity to account termination when there is no longer need for access to the system.

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 contract contains privacy clauses.

☐ 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. *Explanation*

Audit logs are configured to identify, locate and monitor individual activity when using the system. These logs are generated by the components of the MRMSS, and are periodically reviewed and monitored for inappropriate activity. Additionally, access controls restrict and prevent user access to other than "need-to-know" information within the system.

☐ No

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

User actions are monitored to ensure system security. Audit logs are configured to identify and monitor individual activity including user, types of events, dates and times of events, as well as the success and failure of events.

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

Electronic data is protected through user identification, passwords, database permissions and software controls. Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. Audit logs are configured to identify and monitor individual activity including types of events, dates and times of events, and success and failure of events. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

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*

Hard drive encryption (DAR)

(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 Program Manager, Information Management Center, serves as the MRMSS Information System Owner and Privacy Act System Manager, and the official responsible for oversight and management of the MRMSS security and privacy controls and the protection of information processed and stored by the MRMSS system in compliance with Federal laws and policies, and for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system, as well as meeting the requirements of the Privacy Act, in consultation with the ONRR Privacy Officer and DOI Privacy Officials.

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 MRMSS Information System Owner and Information System Security Officer are responsible for managing privacy and security controls, for ensuring to the greatest extent possible that data is properly managed and access to MRMSS is granted in a secure auditable manner consistent with Federal requirements. The Information System Owner/MRMSS Privacy Act System Manager are responsible for ensuring any loss, compromise, unauthorized access or disclosure of PII is immediately reported to the appropriate DOI officials and the Privacy Officer in accordance with Federal policy and established DOI procedures.