**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:** OSMRE Enterprise General Support System (GSS)
**Bureau/Office:** Office of Surface Mining Reclamation and Enforcement (OSMRE)
**Date:** January 9, 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 OSMRE Enterprise General Support System (OSMRE GSS) is a Department of the Interior (DOI) hosted and co-managed Wide Area Network (WAN) backbone supporting the OSMRE user community that provides a secure means of accessing OSMRE working documents and mission related applications, as well as intra-agency service deliveries and access to the Internet

in support of the OSMRE mission. The OSMRE GSS supports the OSMRE user community in performing their duties in support of the Surface Mining Control and Reclamation Act (SMCRA). The OSMRE GSS includes servers, workstations, networking devices (routers, firewalls, switches, and intrusion detection systems), storage, backup devices, and print devices.

The OSMRE GSS is regionally dispersed throughout the United States and is managed at the DOI OSMRE Headquarters (HQ) located at the Main Interior Building (MIB), 1849 C Street, NW, Washington, DC. The OSMRE GSS provides the following services:

- DOI Enterprise Active Directory Service Delivery
- DOI Enterprise Shared Network Service Delivery
- File and Print Services
- Application Hosting
- DOI Enterprise Security and Monitoring Service Delivery

The DOI Enterprise Active Directory (DOI AD) service delivery is an enterprise-wide solution used to provision account management, which includes initial multi-factor authentication leveraging Personal Identity Verification (PIV) card and Kerberos authentication services to provision user permissions, global groups to limit access, and the application of group policies to centrally administer user and computer configuration for OSMRE IT assets. The File and Print Services provides storage for business essential documents in locations that use Microsoft's New Technology File System (NTFS) permissions to restrict access as well as provide a central location for data backup as well as providing a centrally managed print service to print to network resources.

The OSMRE GSS itself does not specifically collect, maintain, or use personally identifiable information (PII) in this system. The OSMRE user community accesses a number of services which may contain PII that are connected to the OSMRE GSS. It is the responsibility of the application system owners, management or personnel accessing the OSMRE GSS to protect the information collected, used, maintained, or disseminated following DOI Rules of Behavior (RoB) guidelines. These services include enterprise office automation software such as Microsoft Office, Adobe products, BisonConnect (Microsoft 365 for Government) and Geographical Information Systems (GIS) and other products that provide access to DOI applications which support Human Resource, Payroll, Finance, Personnel Security, and other functions for OSMRE.

The OSMRE GSS is designed to support the OSMRE mission and may include the transmission, processing, or storage of PII.

OSMRE GSS provides storage repositories that facilitate creation, storage, sharing, and collaborative work for all types of electronic files which may include documents, videos, reports, correspondence, briefing papers, meeting minutes, contacts, grants, permits, audits, manuals, studies, promotional materials, compliance information and other sensitive information. File rights can be delineated to view only and edit/delete and allows staff to share information with professional colleagues as needed. Users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, films, reports, correspondence,

briefing papers, meeting minutes, contacts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that PII may be included in the some of the documents stored. Each user/office program utilizing the OSMRE GSS is responsible for ensuring proper use of the OSMRE GSS and for meeting privacy and security requirements within their department or program areas.

The OSMRE GSS currently supports 2 subsystems that contain PII: (1) E-BUDGET contains information about OSMRE federal employees (individuals) collected from DOI's Federal Personnel and Payroll System (FPPS) that is accessible to limited users and contains specific field identifiers such as name and employee number, and (2) the United Mine Workers of America (UWMA) data which contains information related to beneficiary eligibility of mine workers.

**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 Xacta?**

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

UII Code: 010-000000738, 0730, 0731, 0732, 0733, 0735, 0737, 0739, 0740, 0741, 0743, 0744, 0746, 0747, 0748, 0749, 0750, 0751, 0752, 0753, 0754, 0755, 0756, 0757, 0758, 0759, 0760, 0761, 0762, 0763, 1195, 1228

SSPP Name: OSM Enterprise GSS System Security and Privacy Plan v1.6

☐ 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.* |
|---|---|---|---|
| ArcGIS Image Server | A digital library of raw and processed satellite imagery and derived products and made accessible to multiple users throughout OSM, State, and Tribal offices. | No | N/A |
| Civil Penalty Accounting Information Database (CPAID) | Database used to track the citation and financial data required to approve permits for coal mining operations. | No | N/A |
| E-BUDGET | Internal support system for budget planning and reporting. | Yes | E-BUDGET is an internal OSMRE budgeting application. FPPS data is used to load employee information that includes name, location, DOB, salary, benefits, and step/grade increase. See PIA for E-BUDGET for additional information. |
| Enhanced Abandoned Mine Land Inventory System (EAMLIS) | A system used to store, manage, and report on OSMRE's inventory of abandoned mine land problems. | No | N/A |
| Field Office Comprehensive Information System (FOCIS) | Manages all phases of the Knoxville federal coal program, including permitting, bonding, inspections, etc. | No | N/A |
| Inspection & Enforcement Database (I&E) | National web-based tracking system used to capture and analyze citizen complaints and inspection and enforcement information collected by OSMRE. | No | N/A |

| | | | |
|---|---|---|---|
| National Mine Map Repository (NMMR) | Archives of mine maps for both coal and non-coal mines. | No | N/A |
| INTERIOR/OSM –12, "Blaster Certification" | Manages all phases of the OSMRE federal blaster certification program. | Yes | OSMRE Maintains the records for federal blaster certification in paper files with summary information in an electronic database. See PIA for OSM-12 for additional information. |
| Purchased Evaluated Coal Accumulated Nationally System (PECAN) | Used to store purchased coal tonnage gathered by OSMRE Division of Compliance Management audit staff while they are conducting audits. | No | N/A |
| United Mine Workers of America (UMWA) database | Beneficiary information from the UMWA utilized to correctly validate and pay Surface Mining Control and Reclamation Act (SMCRA) mandated payments to UMWA beneficiaries. | Yes | OSMRE receives beneficiary information from the UMWA via a secured electronic website in order to correctly validate the eligibility of mine workers and authorize payments to UMWA beneficiaries. See PIA for UMWA for additional information. |

**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)*

INTERIOR/OSM-8, Employment and Financial Interest Statements--States and Other Federal Agencies - 64 FR 17412 (April 9, 1999); modification published 73 FR 45244 (August 4, 2008) and 86 FR 50156 (September 7, 2021).

INTERIOR/OSM-12, Blaster Certification – 64 FR 17413 (April 9, 1999); modification published 73 FR 45244 (August 4, 2008) and 86 FR 50156 (September 7, 2021).

Government personnel records are covered by OPM/GOVT-1, Government Personnel Records, 77 FR 79694, December 11, 2012, modified 80 FR 74815, November 30, 2015.

DOI AD records are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); Modification published 86 FR 50156 (September 7, 2021).

DOI employee administrative records are covered by INTERIOR/DOI-58, Employee Administrative Records, 64 FR 19384 (April 20, 1999); Modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021).

DOI employee training records are covered by INTERIOR/DOI-16, Learning Management System, 83 FR 50682 (October 9, 2018).

Other program and user activities that may be subject to the Privacy Act are covered by various government-wide and Department-wide and OSMRE SORNs which are found at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes: *Describe*
☒ No

## Section 2. Summary of System Data

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

☒ Name
☒ Credit Card Number
☒ Employment Information
☒ Other: *Specify the PII collected.*

Although the OSMRE GSS itself does not specifically collect, maintain, or use PII, all these types of PII could potentially exist and be transmitted in the OSMRE GSS. OSMRE GSS transmits DOI AD username(s), work email address(s), work phone number(s), work address(s), DOI employee and contractor titles, and related organizational information required for system administration such as DOI AD information (e.g., username, password, business contact information, etc.), PIV credentials, and security questions and answers to authenticate user identity and to assign permissions to users.

Users may also store all types of electronic files including text, graphical, audio, or video files, which could include documents, forms, reports, correspondence, briefing papers, meeting minutes, contracts, grants, permits, audits, manuals, studies, promotional materials, compliance information, and other documents on the OSMRE GSS IT infrastructure. There is a potential that instances of PII may be embedded in the documents stored. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence and/or comments from members of the public, and other

information related to personnel actions or a specific mission purpose. Forms may collect various types of PII or information on user behaviors. Form owners are responsible for implementing access controls and working with the OSMRE Forms Manager and the OSMRE Associate Privacy Officer (APO) to ensure appropriate authority for the collection, and ensuring that appropriate privacy notice is provided, and privacy risks are addressed.

OSMRE GSS provides hosting infrastructure services to authorized applications and systems within the OSMRE GSS boundary. Please see the applicable privacy impact assessments (PIAs) for the hosted applications and systems for the types of PII and an evaluation of the privacy risks.

**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*

User credentials and authentications are shared with the DOI Active Directory systems.

☒ Other: *Describe*

DOI AD and network infrastructure provides information and services for the purpose of authenticating users and managing access. Initial information is collected by Human Resources (HR) or the Contracting Officer Representative (COR) from individuals during the on-boarding process to establish user accounts. As part of this process, the individual is instructed to complete required Information Management (IMT) Awareness training in security, privacy, records management, Section 508, Controlled Unclassified Information, and Paperwork Reduction Act. Additionally, the user is required to agree to the DOI RoB. Once the training and attestation has been completed the individual forwards a copy of the Certificate of Completion to update the

completion field(s) in DOI Talent, DOI's current Learning Management System (LMS). Human Resources then creates a request which notifies authorized personnel to create the network account(s) for OSMRE GSS. This information is managed in DOI AD and is not collected by OSMRE GSS. IMT training must be repeated and the RoB attested to on an annual basis by all OSMRE employees and contractors.

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

The primary use of the PII is to establish and manage user accounts to enable and maintain authorized access to the OSMRE GSS to accomplish the business-related and mission-related applications used by OSMRE. After establishment of user accounts with username and password, users are required to use PIV credentials to access the OSMRE GSS and DOI network resources. The information is also used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests. This PII is managed in DOI AD and is not collected by OSMRE GSS

Access to OSMRE GSS includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

**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.*

Information may be shared with OSMRE information resource office, human resources, contract management staff or other management staff on a need-to-know basis. The primary use of PII is to enable and maintain authorized access to OSMRE GSS to accomplish the business-related and mission-related applications used by OSMRE. This PII is managed in DOI AD and is not collected by OSMRE GSS

Access to OSMRE GSS includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

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

In the event of a security or privacy event, information may be shared with OSMRE APO or DOI Computer Incident Response Center (CIRC). Information is also shared with DOI to establish user accounts during the on-boarding process opened and managed by DOI Office of the Chief Information Officer.

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

Other Federal agencies do not have direct access to the system. However, data may be shared with other Federal agencies as necessary to meet legal or mission requirements in the course of conducting official business. For example, exchange of communications or information generated from the user community. Authorized sharing with external agencies will be made pursuant to DOI mission authorities and applicable SORNs for each use.

In the event of a security or privacy event, information may be shared with other federal agencies if applicable to a routine use within an associated SORN.

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

Tribal, State or Local Agencies do not have direct access to the OSMRE GSS system. However, data may be shared with Tribal, State or Local Agencies as necessary to meet legal or mission requirements in the course of conducting official business. For example, exchange of communications or information generated from the user community. Authorized sharing with external agencies will be made pursuant to DOI mission authorities and applicable SORNs for each use.

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

OSMRE may contract with other commercial organizations to provide configuration, operations, and maintenance of the OSMRE GSS or specific network components. Contractor staff will be required to undergo background checks as defined by OSMRE and DOI policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system. OSMRE GSS undergoes continuous monitoring by OSMRE and DOI security staff to identify and remediate security vulnerabilities.

☐ 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.*

Information is collected from the individual during onboarding or generated as DOI records (e.g., email address, UPN, username) during operational activities. While the OSMRE HR office completes and submits the required information to create the individual's user account, this information is derived from on-boarding forms. These forms provide the requisite Privacy Act Statement that informs the individual that providing the information is voluntary and the consequences of not providing the information may impact employment.

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

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

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

A Privacy Act Statement is included on the onboarding forms (e.g., OF 306, Declaration for Federal Employment and SF-85P, Questionnaire for Public Trust Positions) which include the requisite information on the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: *Describe each applicable format.*

Users can also view how their information will be used in this PIA, related PIAs, and the SORN's including INTERIOR/OSM-8, Employment and Financial Interest Statements--States and Other Federal Agencies - 64 FR 17412 (April 9, 1999); modification published 73 FR 45244 (August 4, 2008) and 86 FR 50156 (September 7, 2021), INTERIOR/OSM-12, Blaster Certification – 64 FR 17413 (April 9, 1999); modification published 73 FR 45244 (August 4, 2008) and 86 FR 50156 (September 7, 2021), INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), OPM/GOVT-1, Government Personnel Records and other Department-wide, or government-wide SORNs which may be viewed at https://www.doi.gov/privacy/sorn.

☐ 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.).**

Authorized personnel may be assigned permission to view user's account by their name or username within the DOI AD/Enterprise Services. This is typically done at the request of users in order to reset their passwords or to resolve computer and network related issues.

**I. Will reports be produced on individuals?**

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

Automated scheduled and ad hoc reports may be generated to audit user activity and determine accounts which need to be disabled due to employee separation. Data will include name, username, activity date/time, location and applications accessed via OSMRE GSS. Authorized personnel have access to these reports.

☐ No

## Section 3. Attributes of System Data

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

Data is not collected from other sources. The user can only access the OSMRE GSS system as a valid, authorized DOI AD user with current and accurate credentials, an active PIV card, and a valid OSMRE GSS user account.

**B. How will data be checked for completeness?**

Users are responsible for the completeness of the data provided during onboarding and in the user account request form.

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

The OSMRE GSS Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

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

The OSMRE GSS contains a variety of federal records as work products of the users and offices that create them. Records retentions range from temporary review copies to permanent records that will eventually reside in the National Archives. The record schedules consist of General Record Schedules (GRS) maintained by the National Archives and Records Administration (NARA) that pertain to documents that are common throughout the Federal Government. The Departmental Record Schedules (DRS) pertain to records common throughout the DOI and OSMRE specific record schedules under record group 471 that pertain specifically to OSMRE documents

DOI AD records are maintained under the DRS-4.1, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off. Records covered under DAA-0048-2013-0001-0014 also have a temporary disposition and will be cut off when superseded by a newer version or upon termination of the system and destroyed three years after cut-off. Retention periods vary depending on the user created or manage contents and

purpose of the program records. Records created by individual users are retained and disposed of in accordance with applicable Departmental and OSMRE records schedules, or GRS approved by NARA for each type of record based on the subject or function and records series. However, OSMRE has a number of litigation holds in place which may require the retention of these records past the cut-off date.

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

The OSMRE Records Management Exit Clearance process documents the steps and procedures used to remove information when employees and contractors leave the bureau. The records management policies and procedures also govern disposal of information. Procedures for disposition of the data stored in individual applications will vary by program office and needs of the bureau. Due to the nature of the OSMRE GSS, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area. Approved destruction methods for temporary records that have met their retention period include shredding or pulping paper records and erasing or degaussing electronic records in accordance with Departmental policy and NARA guidelines. Permanent records that exist on the OSMRE GSS would be transferred to NARA per their retention schedule.

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

There is a moderate risk to individuals associated with the OSMRE GSS and the hosted applications that reside on the OSMRE GSS due to the potential volume of sensitive PII that may be maintained. OSMRE GSS has a Moderate system security categorization in accordance with NIST standards and Federal Information Processing Standard (FIPS) 199, and the Federal Information Security Modernization Act (FISMA). Multiple controls have been implemented to mitigate and substantially lower privacy risks. The protection and maintenance of information for recovery and backup purposes is done following OSMRE processes for backup and retention of information.

The OSMRE GSS allows the user community to access a number of enterprise services which may contain PII. There is minimal risk to the privacy of official user information throughout the information lifecycle; user information is authenticated by DOI AD for access to OSMRE GSS. Risk is further reduced by following established Office of Management and Budget (OMB), Department of Homeland Security (DHS) and DOI policies, directives, and memorandums. Privacy risk to OSMRE GSS network accounts would affect usernames, passwords and security questions and answers. These risks are mitigated by a combination of administrative, physical, and technical controls.

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which are referenced in the System Security and Privacy Plan (SSPP). Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. The OSMRE GSS SSPP describes appropriate security and privacy controls implemented to safeguard OSMRE GSS 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 SSPP documents the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following OMB, DHS and DOI security and privacy policies, directives. All access is controlled by authentication methods including multifactor authentication (MFA) utilizing PIV cards to validate the authorized user. All DOI employees and contractors are required to complete annual security and privacy awareness training and sign DOI Rules of Behavior. Personnel authorized to manage, use, or operate the system information are required to take additional role-based privacy and security training annually. For the applications hosted by OSMRE GSS, the data is under the control of each program official or system owner who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each 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 OSMRE APO and DOI privacy officials.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Technology is employed to protect information in transit. Data-at-Rest encryption in accordance departmental directive and bureau procedure has been fully implemented for all applicable systems residing in the OSMRE GSS. Other DOI enterprise-level security mechanisms are deployed and actively leveraged to ensure information is safeguarded against potential compromised and unauthorized use.

There is a risk that PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system logs audit trails that can be utilized to protect against unauthorized access, changes, or use of data. Federal employees and contractors are required to take annual mandated security, privacy, and records management as well as role-based privacy and security training where applicable and sign DOI RoB prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update only their working files. For DOI AD user accounts, this risk is further mitigated by validating information against DOI AD leveling PIV authentication.

There is a risk that information in electronic storage will be maintained longer than necessary to achieve the bureau's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with records retention schedules approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. OSMRE Continuity of Operations Plan (COOP), and Business Impact Assessments performed by OSMRE Office of Administration (OA) will define and ensure the ability to recover in the event of improper data disposal.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used, or how to seek access to or connection of their records. This risk is mitigated by the publication of this PIA and related PIAs, applicable SORNs that outline the authority, purpose and uses of information and how individuals can submit requests under the Privacy Act, and Privacy Act Statements provided during the onboarding process or during account creation and activation process. The DOI Privacy Program website also contains DOI and OSM privacy officials' contact information and provides guidance to individuals on how to submit requests or complaints under the Privacy Act.

## 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*

Data collected is required to provide services to enhance productivity and security for the information stored, processed, and transported in support of the OSMRE mission.

☐ 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 OSMRE GSS is not intended to be used in any manner that would allow the system to 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: *Describe*

**H. Authorized Incident Response, and select DOI personnel with a need-to-know may access system or electronic collection How is user access to data determined? Will users have access to all data or will access be restricted?**

Information Owner/Steward grant access in accordance with mission requirements. The principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following OMB, DHS and DOI policies, directives, and memorandums.

For the OSMRE GSS and any associated subsystems, access granted to authorized personnel is enforced with PIV card, MFA, and password. Each person granted access to the system must be individually authorized leveraging two-factor authentication enforcement, to use the system. A Privacy Act Warning Notice appears on the computer monitor screens when a user logs in to the system. Users are only granted access to directories and network locations relevant to their

duties and their particular program areas. Data is protected based on the least privilege principles. All users are required to take annual training in the areas of computer security, records management, and privacy as well as to annually certify the understanding DOI's RoB for retain authorized to DOI and OSMRE service deliveries. Data transmitted between the servers and the endpoints is encrypted.

**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 may be involved in carrying out authorized design and configuration to IT assets residing in the OSMRE GSS. OSMRE GSS System Owner and COR are responsible for approving all contractor led design, testing, deployment, and maintenance any system under contractor control, and must adhere at all times to all Federal laws, regulations, OMB, DHS and DOI policies, directives, and memorandums. Privacy Act contract clauses are included in all contractor agreements in accordance with, and subject to, the Privacy Act of 1974, as amended, 5 U.S.C. 552a, and applicable OSMRE and DOI regulations.

☐ 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*

The purpose of OSMRE GSS is not to monitor individuals, however user actions and use of the system are monitored to comply at all times for security purposes in accordance with OMB, DHS and DOI policies, directives, and memorandums. Information captured include, but is not limited to username, user's last date of login, date of user content creation, date user content was modified or deleted. Additionally, the DOI security network tools include routers, firewalls, and software that log and establish an audit trail of creation and modification of user actions, and the date and time the actions took place. Logs are only accessed by authorized administrative/manager staff. The OSMRE GSS does not actively monitor 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 log records username, date/time, actions. Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and timestamp) for auditing purposes.

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

Access to the OSMRE GSS is only provided to authorized personnel and is applied on the principle of least privilege in order to manage access and log events. Audit features track user activity and record all changes. The OSMRE GSS complies OMB, DHS, and DOI policies, directives and memorandums that are incorporated into the Assessment and Authorization to Operate (ATO). In addition, continuous monitoring along with routine credentialed vulnerability scans of the OSMRE GSS are performed to identify viable weaknesses in the environment. OSMRE GSS maintains an audit trail of activity sufficient to reconstruct security-relevant events. Audit trails include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed as required, and any suspected attempts of unauthorized access or scanning of the system is reported immediately to OSMRE IT Security. Access to administrative functions is strictly controlled. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource.

All OSMRE personnel must complete IT security, records, and privacy awareness training and sign DOI's RoB before being granted access to the OSM GSS, the initial on-boarding process, and at least annually thereafter. All users must annually agree to the DOI RoB.

**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 Mission System Support Branch Chief serves as the OSMRE GSS System Owner and the official responsible for oversight and management of the OSMRE GSS security and privacy controls, including the protection of information processed and stored within the OSMRE GSS. The OSMRE GSS System Owner and OSMRE Associate Chief Information Security Officer (ACISO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for all data stored in the OSMRE GSS. The OSMRE GSS System Owner and OSMRE APO are responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, 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.

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

Data in the applications hosted by the OSMRE GSS is under the control of each relevant System Owner or program official who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including the reporting the loss, compromise, unauthorized disclosure, or access of individuals' personal information, in consultation with the OSMRE APO.

**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 GSS System Owner is responsible for oversight and management of the OSMRE GSS security and privacy controls and for ensuring, to the greatest possible extent, that OSMRE and DOI agency data is properly managed and that all access to data has been granted in a secure and auditable manner. The OSMRE GSS System Owner is 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.

System administrators, employees and contractors are required to report any potential loss or compromise to the OSMRE GSS System Owner, Information System Security Officer (ISSO) and the OSMRE APO.