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: ONRR Mission Support Applications (OMSA)
Bureau/Office: Office of the Secretary (OS), Office of Natural Resource Revenue (ONRR)
Date: April 23, 2025
Point of Contact

Name: Adrienne Brooks-Hill
Title: Associate Privacy Officer
Email: os_privacy@ios.doi.gov
Phone: 202-208-3368
Address: 1849 C Street NW, Rm. 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

X Yes, information is collected from or maintained on

X Members of the general public
X 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 Office of Natural Resources Revenue (ONRR) Web Applications, called the ONRR Mission Support Applications (OMSA), are a group of custom-built web applications used by ONRR staff to support their day-to-day business activities. These tools help ONRR employees track their work, manage cases, maintain electronic records, and support other key functions beyond what is done in ONRR's main system, the Minerals Revenue Management Support System (MRMSS). Each application in the OMSA system is used by different teams for different purposes, such as managing enforcement cases, processing payments, and maintaining records. All applications are used internally by ONRR staff and contractors and require multi-factor authentication. No public-facing websites are included in this system.

These functions include but are not limited to the following: record creation for new leases; reporting and tracking the status of various leases, properties, and royalty payments; enforcement of reporting and payment laws; long term records management; procurement management; employee resources including an organization chart and intranet site; coordination with the US Treasury for delinquent payments; management of appealed orders and demands; and settlement agreements where ONRR is a named party. All applications are accessed using multifactor authentication on an internal network and access is restricted to DOI employees and contractors. There are no public facing web sites in this collection of applications.

This system contains records relating to the general administration of the Minerals Revenue Management Support System (MRMSS), and records relating to minerals revenue asset management, compliance management, and financial management.

C. What is the legal authority?

The Federal Oil and Gas Royalty Management Act of 1982 (FOGRMA), 30 U.S.C. §§1701–1759; Lease, Sale, or Surrender of Allotted or Unallotted Lands 25 U.S.C. Chapter 12, 25 U.S.C. §§ 391–416j; Leases and Prospecting Permits 30 U.S.C. Chapter 3A, 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?

X 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
X Other: *Describe*

The OMSA applications listed at Section 1 part F (20 applications total) are moving from being hosted on government-owned servers (on-premises) to a secure, government-approved Microsoft Azure Cloud environment. These applications support internal operations for Federal employees and contractors. The cloud environment is managed by DOI and meets strict Federal security standards under the Federal Risk and Authorization Management Program (FedRAMP) at the Moderate level. The contract with Microsoft also includes clear requirements to report and respond to any privacy or security incidents.

These applications are hosted on DOI-provided and locally managed Microsoft Azure Cloud resources, which comply with FedRAMP Moderate baseline controls. Incident response responsibilities are defined in the Microsoft Azure Cloud contract, which includes specific provisions for privacy and security incident reporting in compliance with Federal requirements.

E. Is this information system registered in the Bison Governance, Risk and Compliance (GRC) platform?

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

10-000002896; System Security Plan (SSP) for ONRR Mission Support Applications (OMSA) ONRR – Infrastructure – IT Operations and End User Support (OS-0101-MAJ-0101)

☐ 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.*
Appeals Reporting and Tracking (ART)	This web application serves to manage orders, demands, and other actions issued by the ONRR that are subject to appeal. It tracks these appealable items and their associated appeals through the relevant processes.	Yes	Corporate contact information (name, role, email, etc.) A User ID, Name, Organization Code and Supervisor is recorded in association with any entry made in this application.
Budget Tracking Tool (BTT)	The purpose of this subsystem is to house all financial and business data specific to the ONRR organization, as extracted from the Financial and Business Management System (FBMS). It is used to track and reconcile ONRR funding that is not related to payroll.	Yes	User ID, Name, Organization Code and Supervisor is recorded in association with any entry made in this application.
ONRR Company Listing	This application functions as a key subsystem for integrating	Yes	User ID and Name

	and enhancing company data. It pulls foundational information from PeopleSoft and then provides the capability to add valuable, context-specific data, such as identifying related companies, thereby offering a more complete view.		
Data Entry Workload System (DEWS)	The primary purpose of this subsystem is to manage new contracts, including their entry and assignment of work codes. It also tracks the analysts responsible for completing or canceling contracts. Furthermore, the subsystem provides reporting capabilities for both analysts and administrators to monitor team activity and the progress of work.	Yes	User ID, Name, Organization Code and Supervisor
Data Inquiry Reporting Tool (DIRT)	The purpose of this subsystem is to provide a standardized problem report for the entire organization. This report facilitates the identification and escalation of data and data delivery issues to the responsible teams, as well as the Data Governance Board (DBG) and Data Stewardship Council (DSC), enabling proactive management of these issues.	Yes	User ID, Name, Organization Code and Supervisor
Data Intake Solution and Coordination (DISC)	The DISC application functions as a key case management repository. Its purpose is to manage the workflow of cases that begin in PeopleSoft until they are either closed or escalated to	Yes	Corporate contact information (name, role, email, etc.) User ID, Name, Organization Code and Supervisor

	Enforcement and Litigation Support (ELS). Additionally, it serves as a central repository for other relevant datasets not found within PeopleSoft.		
e-Central File Room (eCFR)	The purpose of this subsystem is to provide ONRR personnel with a web-based platform to independently search, track, and request Federal and Indian files. This eliminates the need to visit the central file room for these tasks, streamlining access to essential information.	Yes	Corporate contact information (name, role, email, etc.) Individual Indian Mineral Owner (IIMO) Lease Information and federal and Indian Lease/Agreement information User ID, Name, Organization Code and Supervisor
Enforcement and Litigation Support (ELS)	The primary purpose of the Enforcement and Litigation Support (ELS) application is to serve as the central case management system for the ELS office. It streamlines the management of Enforcement and Bankruptcy cases, other administrative records, and information related to OMB Circular A-123. Additionally, ELS provides reporting capabilities for investigators and administrators to monitor team activity and workload, and it facilitates the generation of reports and documentation for hearings.	Yes	Corporate contact information (name, role, email, etc.) User ID, Name, Organization Code and Supervisor
eRecords	eRecords functions as the Critical Content Management System (CCMS) subsystem for ONRR, providing a centralized platform for managing critical	Yes	Corporate contact information (name, role, email, etc.)

	records. Its primary purpose is to replace the outdated Documentum system. eRecords currently integrates over 1.7 million records from Documentum, in addition to other data sets, and its scope grows as new data sets are incorporated to support various program areas and user group requirements.		Federal and Indian Lease/Agreement information User ID, Name, Organization Code and Supervisor
Indian Daily Estimates and Analysis (IDEA)	The purpose of this web application is to provide ONRR employees with a flexible tool to access and deliver real-time royalty information to mineral lease owners.	Yes	Individual Indian Owner data: contact information (name, phone number); Enrollment ID #; royalty/lease ownership data; profile data User ID, Name, Organization Code, and Supervisor
Individual Development Plan (IDP)	This subsystem is a web-based tool designed to support employee career and personal development. Its purpose is twofold: to facilitate employees in achieving their short- and long-term career goals and to enhance their current job performance. Unlike DOI Talent, this application allows employees to independently identify and request enrollment in specific courses and other career development activities.	Yes	Employee Goals Federal employee employment data, User ID, Name, Organization Code and Supervisor, and other administrative data
Information and Digital Services (IDS) Helping ONRR Personnel (IHOP)	The primary purpose of the Issue Tracker subsystem is to provide comprehensive project oversight. It achieves this by tracking all aspects of a project, including displaying	Yes	User ID, Name, Organization Code and Supervisor

	current tasks, assignments, their status, and essential project details along with any identified issues.		
Market Spatial Analytics (MSA)	This subsystem is designed to oversee and monitor the processing of MSA pricing requests. It tracks each new request from the moment it is submitted until it reaches its final resolution.	Yes	User ID, Name, Organization Code and Supervisor
MRMSS System Change Request (SCR)	The purpose of this subsystem is to allow end users to create and submit change requests specifically for the tools and applications used within MRMSS.	Yes	User ID, Name, Organization Code and Supervisor
ONRR Employee Profile (OEP) - Exit Clearance	The primary purpose of this subsystem is twofold: first, to streamline and manage the Exit Clearance process for departing ONRR Federal employees and contractor personnel. This includes functionality for creating, processing, and tracking clearance requests by ONRR Federal employees, supervisors, and CORs. Second, the subsystem serves as a repository for the ONRR internal organizational chart and general employee data, such as email addresses and phone numbers, for internal reference.	Yes	Federal employee employment data: start date, supervisor, other administrative data User ID, Name, Organization Code and Supervisor
Royalty Overrides in PeopleSoft and eCommerce System (ROPES)	The Royalty Overrides in Peoplesoft and eCommerce System (ROPES) serves as a workload tracking and management subsystem. Its primary purpose is to	Yes	Corporate contact information (name, role, email, etc.)

	streamline the daily tasks of DISC Royalty specialists by providing a central platform for creating and managing override request packets, including the necessary supporting documentation. ROPES also facilitates the review process for DISC supervisors and managers and offers various reports for monitoring team activity and workload.		Federal and Indian Lease/Agreement information User ID, Name, Organization Code and Supervisor
Valuation Tracking Tool (VTT)	The primary purpose of this subsystem is to enable end users to manage project information within the Royalty Valuation system. Specifically, it allows them to add new projects, modify existing project details, and search for projects based on various criteria.	Yes	User ID, Name, Organization Code and Supervisor
Settlements Management and Reporting Tool (SMART)	The purpose of this web application is to manage Settlement Agreements and their impact across various ONRR program areas.	Yes	Named individuals party to a legal Settlement: Name, other similar publicly available information User ID, Name, Organization Code and Supervisor
Strategy Analytics Tracking (SAT)	The purpose of this subsystem is to manage Compliance Review and Audit projects from initiation to completion, and to provide a platform for ONRR program areas to submit and track referrals.	Yes	User ID, Name, Organization Code and Supervisor

Treasury Referral e-Tracking System (TReTS)	This subsystem serves to manage the process of referring items to the Treasury for debt collection. Its functionality includes entering relevant information about these items and subsequently tracking any payments collected by the Treasury.	Yes	User ID, Name, Organization Code and Supervisor

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/OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207 (March 25, 2016); modification published at 86 FR 50156 (September 7, 2021). This SORN may be viewed on the DOI Office of the Secretary (OS) 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*

☒ No

Section 2. Summary of System Data

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

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

This system contains records relating to minerals revenue asset management, compliance management, and financial management. These records are related to business entities and individuals and includes leases, permits, correspondence, forms, disbursements, reports, and other documents which may contain PII including first and last names, address of record for functions addressed, telephone numbers, fax numbers, email addresses, other contact information, lease numbers, revenues collected, outreach information of individual Indian owners, dates due, customer identification number, owner identification number, location of land, type of lease, lessee and/or payor information, allottee production volume, commodity, reported revenues, sales value, royalty amounts, tax identification number, rate billed, amount charged, interest and penalty, collection actions, bank account number, check number, amount paid, contract number, agreement number, allotment number, well number, and other information that may be generated or maintained during the processing and administration of minerals revenue management responsibilities. The records concerning corporations and other business entities are compliance activities and are not subject to the Privacy Act. However, records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information.

ONRR does not intend to collect personal cellular telephone number, home telephone number, personal email address, or home mailing address; however, ONRR may collect those data categories in cases where industry stakeholders are doing business from their homes or are using their personal telephone and/or email address, as sole proprietors, to conduct business with ONRR. The financial information collected by this system consists of royalty reports and payments submitted by industry stakeholders who are responsible for reporting and paying royalties on Federal and Indian energy and natural resource leases. The eCFR, eRecords and ROPES applications hold copies of Leases and Agreements, and multiple financial correspondence records used to establish the legal terms, and a record of compliance activities conducted on these properties by ONRR and ONRR partners, such as the State and Tribal Royalty Audit Committee (STRAC).

ONRR Outreach Program activities include phone calls, email, and correspondence, as well as meetings with individual Indian owners that have ownership in revenues that come from mineral leases. These records may include first and last name, email address, phone number, individual owner identification, allocated ownership percentage, estimated revenues from leases, and other information that may be contained in correspondence with or requests from individuals generated through outreach activities to support and provide a response to customer inquiries.

Individual Indian Mineral Owner (IIMO) data is collected using the IDEA tool, which includes contact information (name, phone number) Enrollment ID number; royalty/lease ownership data and profile data.

ONRR also uses various OMSA applications to collect employee information, from the education/training goals, and employment data including key employment dates, chain of command, and other administrative data in that is contained in IDP and the OEP.

The SMART application tool tracks named individuals party to a legal settlement.

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*

The ONRR collects PII from individual industry participants through our website or paper forms. We will also move existing PII data into our new system (OMSA) from ONRR's older computer systems, including those used for financial information, data analysis, and compliance. This older data was also originally collected from individuals.

The OMSA system is only for ONRR staff to use internally. It works by copying information from other ONRR computer systems that receive data from forms. These forms include production reports, royalty information, and forms like the "Addressee of Record Designation" (ONRR-4444) and the "Designation Form for Royalty Payment Responsibility" (ONRR-4425). Other information is also submitted through different systems, such as our public website (onrr.gov, which is separate from OMSA) or systems used by other government agencies like the Bureau of Indian Affairs (BIA) or the Bureau of Trust Funds Administration (BTFA). The OMSA system then copies this information into specific internal applications where ONRR staff can manage and process cases as needed. These individual case management applications are also separate from the main OMSA system. Therefore, the entire OMSA system is designed for internal ONRR use only.

Besides the official reporting forms submitted through onrr.gov, data can also get into the OMSA system in other ways. This includes receiving data from other agencies like the BIA or BTFA, receiving information as email attachments (for example, a company sending a formal appeal that is then added to a case file), and when individuals or companies call ONRR and provide information about their case, profile, or lease (this information is then typed into the system by an ONRR employee).

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 Some OMSA systems transfer data to other ONRR systems to complete ONRR business functions.
☒ Other: *Describe*

OMSA does not broadly collect information from the public via forms, surveys, or similar mechanisms.

Authorized ONRR users have access to the BTFA Indian Trust Systems Query (ITSQ) containing information from the BIA Trust Asset and Accounting Management System (TAAMS), the system of record for title and land resource management of Indian Trust and Restricted Land with DOI and BIA, to manually retrieve data regarding lease ownership of the Individual Indian Mineral Owner (IIMO). The information for IIMO is transferred manually and kept in a paper file. IIMO paper forms are maintained in a physical secure file room at ONRR's Denver Federal Center location. The Denver Federal Center has security guards, and the locked file room is in a secured facility requiring identification badges, and key card access. The paper forms are converted digitally into ONRR's electronic record management system and are dispositioned in accordance with the applicable DRS records schedule.

The ONRR Modernization system is building a Customer Relationship Management (CRM aka "ONRR Connect") capability, which will allow data flow between multiple ONRR systems (including OMSA applications) to complete ONRR business functions.

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

- The PII data is used to contact industry stakeholders in relation to their responsibility to:
  - report and pay royalties on Federal and Indian energy and natural resource leases and
  - report production on Federal and Indian energy and natural resource leases in support of ONRR's mission to collect, account for, and verify natural resource and energy revenues due to States, American Indians, and the Treasury.
- PII data is used internally to manage employee and contractor administrative data. This includes:
  - training goals by an employee and supervisor and other employment administrative data
  - company contact information, named individuals on a settlement, and financial correspondence records
- Indian mineral lease owner PII is used to provide real time royalty information and for communication and includes contact information, enrolment IDs, royalty/lease ownership data and profile data.

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.*

All applications listed as OMSA applications are used internally by ONRR. These tools are designed to meet specific business needs, including managing royalty payments, processing appeals and settlements, managing employee data, and verifying payments from energy production on Federal and Indian lands. Before anyone is granted access to the OMSA applications, their request is reviewed and approved by system owners and documented according to DOI access control policies. Access is limited to individuals who need the information to perform their official duties. This ensures that personal information is only shared with authorized users who have a valid business need. PII is shared within ONRR and, when necessary, with other DOI offices, federal agencies, Tribal, State, and local agencies, and contractors. Any external sharing follows the routine uses listed in the published System of Records Notice (SORN).

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

Access requests, both internal and external, are reviewed and documented in accordance with DOI access control policies. Approval is required by system owners, and access is restricted to authorized users with a need-to-know basis. A formal approval process is in place to ensure only properly authorized individuals are granted access to PII in the OMSA applications.

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

All applications listed as OMSA applications are for internal ONRR use. However, we may share information with bureaus, such as BIA, Bureau of Land Management (BLM), Bureau of Ocean Energy Management (BOEM), Bureau of Safety and Environmental Enforcement (BSEE) and federal agencies such as U.S. Government Accountability Office (GAO), Department of Justice (DOJ), Office of Inspector General (OIG), and other agencies that have a stake in either a litigation, joint investigational work related to the management of mineral production and revenues.

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

ONRR may share information with other Federal agencies in the performance of their duties. PII may also 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. Disclosures made outside of DOI are outlined in the routine uses in INTERIOR/OS-30, Minerals Revenue Management Support System (MRMSS), which may be viewed on the OS SORN website at https://www.doi.gov/privacy/os-notices.

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

ONRR may share industry stakeholder information with ONRR's State and Tribal Royalty Audit Committee (STRAC) partners when auditing reporting and payments. Information may be shared with Tribal, State or local agencies when authorized or required by law, as outlined in the routine uses in INTERIOR/OS-30, Minerals Revenue Management Support System (MRMSS), which may be viewed on the OS SORN website at https://www.doi.gov/privacy/os-notices.

☒ 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 OMSA 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 INTERIOR/OS-30, Minerals Revenue Management Support System (MRMSS), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/os-notices.

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 conducting royalty payment activities, following up regarding royalty-related issues of interest to the individuals, and to process bonuses, rents, and royalties received from mineral leases on Indian land. Failing to provide this information will prevent ONRR from disclosing payment information.

☐ 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 Act Statement: This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Authority: This information is being solicited under the authority of The Federal Oil and Gas Royalty Management Act of 1982, 30 U.S.C. 1701-1759; Chapter 12 of Title 25 of the U.S. Code, addressing the lease, sale, or surrender of allotted or unallotted lands, found at 25 U.S.C. 391-416j; Chapter 3A of Title 30 of the U.S. Code, 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. Purpose: The primary purpose for collecting this information is to collect royalties and rents; control revenues; distribute funds collected; maintain records of royalty accounts and associated sales, and production information. Routine Uses: The routine use of this data is 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. Citation: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as found in the published system of records notice, Minerals Revenue Management Support System (MRMSS), OS-30 (Replaces MMS-1) - March 25, 2016, 81 FR 16207, which may be viewed at: https://www.govinfo.gov/content/pkg/FR-2016-03-25/html/2016-06813.htm. Furnishing the information on the form is voluntary; however, failure to provide the mandatory information required by the form and 30 C.F.R. § 1210.52(a) (1-10), will prevent a lessee from designating a person to make royalty payments on its behalf. See 30 U.S.C. § 1712(a); see also 30 C.F.R. §1210.158"

☒ Privacy Notice: *Describe each applicable format.*

Individuals are also provided notice on how their personally identifiable information (PII) is managed within OMSA through the publication of this PIA and the INTERIOR/OS-30, Minerals Revenue Management Support System (MRMSS), SORN. The SORN can be reviewed at https://www.doi.gov/privacy/os-notices.

☒ Other:

Employees and contractors receive a warning that informs users 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.).

Customer records are retrieved by name or customer identification number (ONRR unique identifier), owner name, or owner identification number. Land information is retrieved by location and whether the lease is an Indian lease or a Federal onshore or offshore lease. Records are indexed by lease or contract number; lessee and/or payor; permittee; production reporter; and/or commodity. Individual Indian Mineral Owners have a unique enrollment ID number verified to their name.

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 IIMO leases. Reports are viewed on screen and only printed when extenuating circumstances require further analysis. The printed report is kept in a locked paper file. ONRR employees supporting IIMO have access to the paper files and they are only shared with the specific IIMO.

Reports run for project, budget, travel, system updates, contractor and training may run on individuals. These reports support the operation and management of resources such as money, inventory, employees, and contractors. ONRR employees and contractors with responsibilities to manage the (project, budget, travel, system updates, contractors, and training) have access to these reports.

The system will include audit logs documenting user access and activity within the system. These logs will be available to the designated DOI personnel responsible for reviewing audit log data. The audit logs will contain details relating to the use of the system, including username, date/time, user's last date of login, failed login attempts, data/reports accessed, and

data exported.

☐ 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 IIMOs is collected from the IIMOs directly, so it is assumed to be correct at the time of collection and is not further verified for accuracy.

For data transferred from other systems to OMSA applications that are provided from other bureaus or agencies, ONRR will collaborate with other DOI agencies (BLM, BSEE, BIA, etc.) to resolve any discrepancy or potential inaccuracies identified during ONRR's review of the data. Royalty and Production reports are validated upon receipt from industry participants through a series of up-front edits that flag reports with obvious errors. When these errors are flagged, ONRR works with the industry participants and directs them to correct the reporting.

B. How will data be checked for completeness?

For data transferred from other systems to OMSA applications, the original ONRR receiving system will prompt industry stakeholders to certify that the data they are submitting is accurate, compete and up to date. ONRR receives a signature certification for email and paper form submissions. Submissions for Forms ONRR-4444 and ONRR-4425 are reviewed for completeness by ONRR.

Certain OMSA applications use electronic forms, which helps to ensure that all necessary fields have information and depending on the field, the correct type of data format. Data input into

OMSA applications is reviewed for proper routing and handling when the request is sent to appropriate team.

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

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

The OMSA system receives company information from other Department of the Interior (DOI) agencies like the BLM, BSEE, and BIA. These agencies are responsible for keeping the information up-to-date about the companies that handle reporting and payments for energy and natural resource leases. For the data within OMSA itself, the system updates every hour. This means that any new company information or changes made in the other DOI systems that OMSA uses will appear in OMSA within one hour. The same hourly update applies to any manual changes made to OMSA data by an ONRR employee; these changes will be reflected in the system after the next hourly refresh.

For contact-level data, ONRR relies on the industry stakeholders to maintain data describing who within their company is currently responsible for interactions related to their company's reporting and payment responsibilities.

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 kept according to an approved records schedule by the National Archives and Records Administration (NARA). Some records must be kept permanently, while others are temporary and will be deleted after a set period. Most temporary records will be kept for seven to ten years, depending on their type, unless they are subject to a litigation hold. When records are no longer needed, they will be securely deleted or transferred to NARA.

Administrative records and general correspondence files have temporary dispositions and are maintained in accordance with 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 Federals Records Center, one year after cutoff, and eligible to be destroyed 7 years after cutoff, providing no records holds on litigation holds are in effect.

A new Departmental Records Schedule (DRS), Mission Schedule 2-2 is pending NARA approval will replace certain items on the current NCI-057-84-07 schedule. The disposition for most federal temporary records is 10 years after cut off. The disposition for permanent records will be transferred to NARA.

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

When the PII is no longer relevant and/or necessary, the paper and electronic information will be dispositioned in accordance with DRS, Mission Schedule 2-2. An inventory of the information that would be deleted is captured on form DI-1941 (Documentation of Temporary Records Destruction) and signed by the system owner and the Records Officer. The documented procedures for the deletion of information are under Departmental Policy Royalty Management Program 2020-03 Federal Records Disposal Authorization.

For data that has a permanent retention, all information will be maintained electronically (either captured in native software or converted digitally) and submitted to NARA Electronic Records Archive (ERA). The procedure for transferring electronic records is under Department Guide RMG-2020-00 (Departmental Records Schedule Implementation Guide).

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.

The OMSA system has identified privacy risks that could affect individuals whose information is in the system. These risks include the possibility of unauthorized access to personal information, accidental disclosure, errors in who has access, and delays in removing access when someone leaves ONRR. Additionally, since the system is cloud-based, there is a risk if the cloud provider does not follow privacy rules.

To reduce these risks, OMSA uses strong privacy and security protections:

a. Access is limited to authorized ONRR employees and contractors who need the information.
b. User activities are monitored through audit logs.
c. The system follows federal privacy and security laws, including the Privacy Act, FISMA, and NIST standards.
d. Physical, administrative, and technical safeguards are in place to prevent unauthorized access.

Records are kept only as long as required and then securely deleted.

These risks are mitigated by the controls implemented to safeguard PII and secure the network 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. OMSA applications are compliant with the Privacy Act of 1974, Federal Information Security Modernization Act of 2014 (FISMA), Joint Financial Management Improvement Program (JFMIP)/Federal Accounting Standards Advisory Board (FASAB), 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 current revisions of NIST Special Publication 800-53, 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.

PII and other sensitive data is protected through access 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 their 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 initial and annual security, privacy, and records management awareness training, as well as role-based privacy and security training, and sign the DOI Rules of Behavior.

Users are trained not to share or publish sensitive data with unauthorized parties. OMSA applications employs sensitive data classification for user awareness and the system administrators periodically review user content to ensure compliance with DOI security and privacy policies. Records are maintained and disposed of under a NARA approved records schedule. Information collected and stored within the OMSA is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Individuals are provided notice through the publication of this PIA and INTERIOR/OS-30 SORN. A Privacy Act statement is provided on the ONRR-4425 form. If a user were to use Login.gov, notice is also provided to Login.gov users through the GSA Login.gov PIA and GSA/TTS–1 SORN. Once the Authority to Operate is completed, ONRR will move from the current on-premise domain authentication to an Azure hosted Entra authentication.

Data provided by customers are reviewed to ensure they are accurate and complete. Inaccurate or incomplete data is identified by the system and/or ONRR technicians and corrected.

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*

ONRR collects, accounts for, and verifies energy and natural resource revenues. ONRR distributes the revenues to States, American Indians, and Treasury. The collection of and verification of these revenues requires ongoing communication between ONRR and the industry participants who are responsible for reporting and payment. ONRR must collect and maintain contact data for these industry participants to ensure ONRR is able to carry out these communications effectively and efficiently. ONRR as an organization needs to manage employees, contractors, projects, systems and training and the valuable resources entrusted to it, such as the budget. These systems also help to ensure that users can access and find data to complete their assigned projects. In particular, the OMSA IDEA application is critical in assisting ONRR with the import role with IIMOs.

☐ 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. OMSA applications do 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*

Access to OMSA data is limited to ONRR employees, contractors, system administrators, and developers. Everyone who accesses OMSA must use a government-issued device and log in with a Personal Identity Verification (PIV) card. Access is restricted to what the person needs to do their job.

Internal users will be granted access to data based on their role in the organization. Most internal users will have read-only access to customer data; a small number of internal users will be able to add/edit customer data to account for the fact that ONRR sometimes receives that data on paper forms that must be entered into the OMSA applications.

Contract developers will be treated similarly to internal users in that they will be required to access the system using GFE and their PIV.

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

Users are assigned specific roles based on what they need to know. They only have access to the information necessary to perform their job duties. For example, most users will have "read-only" access, while some authorized staff may be able to enter or update data.

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?*

Yes, the contract includes all required IT Security, Privacy, and Records clauses as mandated by both government-wide and DOI policy. This specifically includes Privacy Act contract clauses, as well as privacy terms and conditions and the applicable privacy FAR clauses. These provisions ensure that privacy and other relevant regulatory measures are addressed.

☐ 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*

Interactions and other user activities within the OMSA applications are tagged with the name of the user as part of the audit logs. Additionally, access controls restrict and prevent user access to other then “need-to-know” information within the system.

☐ No

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

Information collected includes the name of the user and maintenance of an audit log of their interaction within the system, which consists of:

* Log on attempts (successful or unsuccessful);
* Dates and times of events;
* Function(s) performed after logged on (e.g., reading or updating critical file, software installation);
* Account changes (e.g., account creation and deletion, account privilege assignment), and
* Successful/failed use of privileged accounts.

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

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. 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 are required to review these audit logs and ensure that only authorized personnel who have a need to access the audit records in the performance of their official duties are accessing these records. System administrators prevent unauthorized monitoring by protecting data through user identification, passwords, database permissions and software controls.

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*

OMSA inherits all physical controls of the FedRAMP-authorized cloud service provider. The entire system is cloud-hosted in third party owned and managed facilities, and there are no paper records kept within the OMSA system.

Paper forms are maintained in a physical secure file room at ONRR's Denver Federal Center location. The Denver Federal Center has security guards, and the locked file room is in a secured facility requiring identification badges, and key card access. The paper forms are converted digitally into ONRR's electronic record management system and are dispositioned in accordance with the applicable DRS records schedule.

(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 Program Manager, Information & Digital Services, serves as the oversight and management of the OMSA security and privacy controls and the protection of information processed and stored by the OMSA system. The Information System Owner, Information System Security Officer (ISSO), and Privacy Act System Manager are responsible ensuring adequate safeguards are implemented for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system, in compliance with Federal laws and policies, as well as meeting the requirements of the Privacy Act, in consultation with the Office of the Secretary (OS) Associate Privacy Officer (APO) and ONRR Privacy Official.

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 OMSA Information System Owner and ISSO are responsible for managing privacy and security controls, for ensuring to the greatest extent possible that data is properly managed and access to OMSA is granted in a secure auditable manner consistent with Federal requirements. The OMSA Information System Owner and Privacy Act System Manager are responsible for ensuring any loss, compromise, unauthorized access to or disclosure of PII is immediately reported to DOI-CIRC, DOI's incident reporting portal, within 1- hour of discovery and the appropriate DOI officials, including the OS APO and ONRR Privacy Official, in accordance with Federal policy and established DOI procedures.