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: Automated Fluid Mineral Support System
Bureau/Office: Bureau of Land Management
Date: May 22, 2023
Point of Contact:
Name: Catherine Brean
Title: BLM Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: 830-225-3459
Address: Bureau of Land Management, 1849 C Street NW, Room No. 5644, 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

B. What is the purpose of the system?

The BLM manages the Federal government's onshore subsurface mineral estate – about 700 million acres (30% of the United States) held by the BLM, U.S. Forest Service and other Federal agencies and surface owners for the benefit of the American public. The Automated Fluid Mineral Support System (AFMSS) is an enterprise application that facilitates the collection, management and sharing of authorized use regulatory fluid mineral permits/reports

and field operations data across Federal onshore operations including Indian Trust Lands. It contains data concerning lease and agreement ownership, well identification, location, and history, including casing information, geologic formations, resource protection, production, approvals of operations bond and surety information, and operator compliance. The system has an electronic commerce module, the Application for Permit to Drill (APD) module, to interface with the oil and gas industry. Industry also utilizes the Sundry module and Well Completion Reports module to report activities and receives communication from the Inspection and Enforcement Module. AFMSS was built in 1997 and due to aging technology was completely upgraded in 2021. All data from the legacy system was migrated into the new version of AFMSS currently in production.

The personally identifiable information, PII, stored in AFMSS includes the following:

- Contact information for an Operator, Third Party or Lessee, grouped by case number, is entered/stored in the AFMSS enforcement screen by a BLM employee. Generally, the contact information is company information, but it could be an individual operating their own business using their personal information which constitutes PII. The BLM employees collect this information so the system can generate, and track notices, such as a Notice of Non-Compliance, sent out to the appropriate contact.
- Private Surface Owner Contact Information: Onshore Order 1 requires the operator to submit the name, address, and phone number of the surface owner, if known, in its APD. While AFMSS no longer directly captures PII for the private surface owner, operators may include that information in an attachment as part of their application. The operator will usually make an agreement with the surface owner for access. However, the operator has the option to post a bond if he is unable to reach an agreement.
- AFMSS stores the names of BLM employees that perform inspections, as part of their official work duties, on the cases so that a supervisor can be assigned to their work to oversee it and so their names appear on Enforcement Action forms. Inspections include oversight done by an employee's supervisor. This includes the employee's name and the type of inspection that is being oversighted. The information that is related to the employee's job performance is not captured in AFMSS.
- The Operators (Oil and Gas Companies) are required to supply a business email, business address, business phone number, and name to create an AFMSS account to apply for permits and submit Sundry Notices and Well Completion Reports.

C. What is the legal authority?

- Minerals Lands and Mining (30 U.S.C. 39, 181, 201)
- Bureau of Land Management, Minerals Management (43 CFR 3000)
- Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.)
- Federal Land Policy and Management Act (43 U.S.C 1701 et seq.)
- Uniform Relocation Assistance and Real Property Acquisition Policies Act (42 U.S.C 4601)

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

E. Is this information system registered in CSAM?

☒ Yes

The UII Code is 010-000000086 and the SSP is AFMSS System Security and Privacy Plan.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

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

☒ Yes

INTERIOR/LLM-32, Land & Minerals Authorization Tracking System, 56 FR 5014 (February 7, 1991), modification published at 73 FR 17376 (April 1, 2008) and 86 FR 50156 (September 7, 2021) is currently being revised to incorporate four SORNs into one program area and will include:

- BLM-3, Mineral Lease Management – 47 FR 55317 (December 8, 1982); modification published 73 FR 17376 (April 1, 2008), and 86 FR 50156 (September 7, 2021)
- BLM-4, Coal Lease Data System, 47 FR 43317 (December 8, 1982); modification published 73 FR 17376 (April 1, 2008), and 86 FR 50156 (September 7, 2021)
- BLM-6, Mineral Surveyor Appointment File – 51 FR 25107 (July 10, 1986); modification published 73 FR 17376 (April 1, 2008), and 86 FR 50156 (September 7, 2021)

The consolidated revision will update all sections of the notice to incorporate information pertaining to the consolidated system of records effort, to include a new routine uses and include simplified formatting of the previously published notice to reflect updates consistent with the

DOI standard routine uses in accordance with the Office of Management and Budget (OMB) policy.

☐ No

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

☒ Yes

Data is input into this information system using forms requiring OMB approval and assigned OMB Control Numbers. The information maintained in AFMSS is collected on the following forms and their designated OMB Control Number:

OMB 1004-0137, Onshore Oil and Gas Operations and Productions (43 CFR 3160 and 3170). The expiration date is January 1, 2025.

- Form 3160-3, Application for Permit to Drill or Re-enter
- Form 3160-4, Well Completion or Recompletion Report and Log
- Form 3160-5, Sundry Notices and Reports on Wells

☐ No

Section 2. Summary of System Data

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

☒ Name
☒Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address

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

Private Surface Owner Contact Information: Onshore Order 1 requires the operator to submit the name, address, and phone number of the surface owner, if known, in its Application for Permit to

Drill (APD). While AFMSS doesn't directly capture PII from the private surface owner, operators may include that information in an attachment as part of their application.

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

The application utilizes Login.gov for identity and authentication functionality for external users. Internal users leverage Single Sign On (SSO) which authenticates them using Personal Identity Verification (PIV) credentials against the BLM AD. External users leverage a username and password to authenticate into the system. All external user accounts are first created in Login.gov SSO to support authentication, and then created in the AFMSS application for authorization. Each AFMSS User account is tied to a BizFlow (Commercial off the Shelf) license type, which controls the level of access and permissions a user will have within the application. The General Services Administration (GSA) manages Login.gov and privacy risks are addressed in the Login.gov PIA, which may be viewed on the GSA PIA website.

☒ Other

Some contact information stored in AFMSS comes from another BLM application. Federal employees will look up lease owner information that is stored in BLM's Minerals and Lands Records System (MLRS) and manually enter the contact information into the Lessee contact screens in AFMSS. There is no connection or information sharing between AFMSS and MLRS. MLRS, is a system that contains data about land and mineral use authorizations (permits, O&G leases, Rights of Ways, mineral leases, etc.), land title, (exchanges, acquisition, conveyances, etc.), and segregation (withdrawals, classifications).

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

The PII in AFMSS is used to contact key personnel involved in the Oil & Gas operations to make arrangements for private property access, communicate inspection and enforcement findings, and to provide multiple types of notifications.

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

☒ Within the Bureau/Office:

The PII is shared within the Bureau as federal users can view all Oil and Gas contacts for communication purposes. Most correspondence is automated through the AFMSS system however, the federal user may contact them via email or phone call.

☒ Other Bureaus/Office:

BLM AFMSS shares system data with the Office of Natural Resources Revenue (ONRR) through a schedule process. Approved users from ONRR and the Bureau of Indian Affairs' (BIA) have accounts and access to the AFMSS application and data.

☒ Other Federal Agencies:

AFMSS has a Memorandum of Understanding (MOU) with the U.S. Department of Agriculture (USDA) Forest Service (FS) covering oil and gas leasing and operations. This MOU satisfies requirements of Section 363 of the Energy Policy Act of 2005, PL I 09-58 (the Act), which directs the Secretary of the Interior and the Secretary of Agriculture to enter into a memorandum of understanding regarding oil and gas leasing on public land under the jurisdiction of the Secretary of the Interior, and on FS land under the jurisdiction of the Secretary of Agriculture. This MOU allows FS users access to the BLM AFMSS application and data. BLM provides user accounts in AFMSS to approved USDA FS users so they can access core data stored within the system. The purpose of this access is to perform activities related to surface inspections if a well contains USDA FS managed land.

☐ Tribal, State or Local Agencies:

☒ Contractor:

There are BLM contractors who provide development, operations, and maintenance support to the AFMSS application.

☐ Other Third-Party Sources:

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

☒ Yes:

An agreement is established between the Operator and the private surface owner as a third-party activity. At that time, the private surface owner could opt out of providing PII to the Operator; the contact information would not be entered into AFMSS and BLM could not contact the surface owner to validate an existing agreement is in place. The operator will usually make an agreement with the surface owner for access. However, the operator has the option to post a bond if they are unable to reach an agreement. All official forms have the privacy act notice included to ensure users understand their right to decline or consent to specific users of PII data.

☐ No:

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

☒ Privacy Act Statement:

In accordance with OMB Circular No. A-108, the BLM 3160-3, 3160-4, and 3160-5 forms all contain a Privacy Act statement which provides sufficient information about the request for information as it pertains to the application process.

☒ Privacy Notice:

Notice is provided through the publication of this PIA. Notice is also provided through the publication of INTERIOR/ LLM-32, Land & Minerals Authorization Tracking System SORN. The INTERIOR/LLM-32 SORN is currently under revision as described above in Section 1.G of this PIA.

☒ Other:

When users log into AFMSS they do so by first accessing the login screen which has a hyperlink to the DOI Privacy Policy page.

☐ None

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

The Application Permit to Drill (APD) Number is used to retrieve information associated with the permit including the surface owner if provided in the application as an attachment by the operator, and the case number and operator combination is used to retrieve the group of contacts for the well. The system does not have the ability to retrieve information associated with an individual since there is no unique identifier tied to the record for that person.

I. Will reports be produced on individuals?

☐ Yes:

☒ No

Section 3. Attributes of System Data

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

The information maintained in AFMSS is collected from the third-party source and not directly from the individual. The BLM does verify the data submitted by the permit applicant as the BLM contacts the surface owner to ensure an operating agreement with the operator is in place and to invite them to the onsite inspection of the proposed well. If the information provided by the operator is inaccurate, the person the BLM erroneously contacts could inform the BLM that they do not have record title to the surface rights. The BLM would then either go back to the permit applicant to have the operator update the information or search publicly available data

such as the county assessor's records to obtain record title owner of the surface rights. If information from a third-party system, such as MLRS, appear to be incorrect, the person that identified the error would contact the system User Representative to let them know about the possibility of an error in the record.

B. How will data be checked for completeness?

AFMSS does not collect PII data from the individual directly. Since PII data stored in AFMSS is shared from another BLM system (MLRS) and third-party sources, it is the responsibility of the source at the initial point of collection to ensure that PII data provided is correct, accurate, and complete prior to entry into the AFMSS System. If an AFMSS user performing data entry identifies an error with the third-party data, they would notify the third-party source of the error. An AFMSS BLM [Federal] user is responsible for data entry from a third-party source. If a data completeness issue is identified from the third-party system, the AFMSS BLM [Federal] user would contact the third-party system [Federal] Support Team of the issue.

When an Operator submits a new account request to the AFMSS BLM User Support Team (documented via Help Desk ticket), the information is manually reviewed for completeness. If there is incomplete information provided to BLM in the new account access form, the AFMSS User Support Team reaches out to the submitter directly via email or phone call to get any incomplete data. The AFMSS system requires the following data (business name, business email address, business address, and business phone number) to create an account. Within the AFMSS system, these fields are required to ensure completeness of data entry

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

AFMSS does not collect PII data from the individual directly. Since PII data stored in AFMSS is shared from another BLM system (MLRS) and third-party sources, it is the responsibility of the source at the initial point of collection to ensure that PII data provided is correct, accurate, updated, and complete prior to entry into the AFMSS System. If an AFMSS user performing data entry identifies an error with the third-party data, they would notify the third-party source of the error. An AFMSS BLM [Federal] user is responsible for data entry from a third-party source. If a data completeness issue is identified from the third-party system, the AFMSS BLM [Federal] user would contact the third-party system [Federal] Support Team of the issue.

For user account information stored within the system, the AFMSS User Support team conducts routine account audits to ensure data is current and accurate. If user account information is not current, accurate, or no longer a valid account, the AFMSS User Support Team takes corrective actions to update account information in the system. If there are changes to the user account information, a new 1260-12 form is required to be submitted. If an internal user account is disabled or no longer in Active Directory, then the AFMSS User Support team would disable that account in the AFMSS system.

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

AFMSS records are covered under the approved Department Records Schedule (DRS)/General Records Schedule (GRS)/BLM Combined Records Schedules which is a combination of schedules developed by the National Archives and Records Administration (NARA), the Department of the Interior (DOI) and the Bureau of Land Management (BLM). AFMSS has a combination of Permanent and Temporary records. The breakdown is as follows.

The following records in AFMSS are PERMANENT. These records are retained and transferred to NARA in accordance with DRS/GRS/BLM Combined Records Schedule disposition instructions. COMMUNITIZATION, UNITIZATION, GAS STORAGE, AND SPACING ORDER FILES- Indian Agreements (schedule 4/26b(1)); OIL AND GAS LEASING FILES - Oil and Gas Operations Lease and Well Files – Indian (schedule 4/27b(1)); OIL AND GAS LEASING FILES- Oil and Gas Development Map Masters (schedule 4/27e); OIL AND GAS LEASING FILES - Oil and Gas Production Accountability Review Files - Indian Trust Lands (schedule 4/27i(2)).

The following records in AFMSS are TEMPORARY. These records are retained and disposed in accordance with DRS/GRS/BLM Combined Records Schedule disposition instructions. COMMUNITIZATION, UNITIZATION, GAS STORAGE, AND SPACING ORDER FILES - Federal Agreements (Schedule 4/26b(2). Records are transferred to the FRC 10 years after established cutoff. FRC will destroy 75 years after cutoff.

OIL AND GAS LEASING FILES - Oil and Gas Operations Lease and Well Files – Federal (Schedule 4/27b(2). Lease and well files will be transferred to the FRC 10 years after the established cutoff. FRC will destroy 75 years after cutoff.

OIL AND GAS LEASING FILES - Individual Well Records (IWR) and Scout Tickets (Schedule 4/27g); Retention - Destroy when superseded, obsolete, or no longer needed for reference.
OIL AND GAS LEASING FILES - Oil and Gas State Lease and Well Reference Copies (Schedule 4/27h). Records will be destroyed when superseded, obsolete, or no longer needed for reference.

OIL AND GAS PRODUCTION ACCOUNTABILITY REVIEW FILES - Oil and Gas Production Accountability Review Files - Federal Lands (Schedule 4/27i(1)). Records will be transferred after completed review to the FRC 3 years after the established cutoff. FRC will then destroy 8 years after cutoff.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy apply to COMMUNITIZATION, UNITIZATION, GAS STORAGE, AND SPACING ORDER FILES - Federal Agreements (Schedule 4/26b(2); OIL AND GAS LEASING FILES - Oil and Gas Operations Lease and Well Files – Federal (Schedule 4/27b(2); Individual Well Records (IWR) and Scout Tickets (Schedule 4/27g); Oil and Gas State Lease and Well Reference Copies (Schedule 4/27h); and OIL AND GAS PRODUCTION ACCOUNTABILITY REVIEW FILES -

Oil And Gas Production Accountability Review Files - Federal Lands (Schedule 4/27i(1) records due to the fact they are TEMPORARY records.

The procedures for AFMSS files documented in BLM Records Retention Catalog Schedule 4/26b-26b(1); 4/27b(1); 27e; and 27i(2) are PERMANENT. Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA Guidelines.

Permanent records are never destroyed and are always identified for transfer to NARA at a specific time after cutoff.

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

There is a privacy risk due to the type and volume of personal information maintained in AFMSS. Operators submit Applications for Permit to Drill (APDs) associated with existing federal and/or Indian oil & gas leases. Where a proposed well is located on privately owned surface, the application should include contact information for the private owner, including name, address, phone number(s), and email address(es). The only users that need access to this information are inspectors who will invite the surface owner(s) to participate in inspections that include their lands. To mitigate privacy risk, BLM has restricted access to PII within AFMSS to authorized users.

There is a risk that individuals may gain unauthorized access to the information in the system. System security controls are in place to prevent access by unauthorized individuals to sensitive information. AFMSS is classified as moderate for FISMA and has all the required security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, AFMSS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of passwords, user identification, IP addresses, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use AFMSS or those who do not have a direct "need to know" certain information contained in AFMSS. All end-users have an individual password and ID. All new users receive training on and there is a user guide detailing the appropriate use of AFMSS. All DOI employees and contractors must annually complete mandatory privacy, security, and records management training, including role-based privacy and security training, and acknowledge the DOI Rules of Behavior.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting, and sharing information with unauthorized recipients, or used for an unauthorized purpose. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties. Access to information is role-based and is only granted on a need-to-know basis and requires DOI credentials. Accounts are reviewed annually to ensure that only authorized personnel have AFMSS logins. Additionally, any account that is

inactive for more than one year is automatically suspended. All personnel accessing AFMSS must acknowledge the rules of behavior prior to each login. The System Security and Privacy Plan per BLM Policy maintain a record of activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Activities are also captured within AFMSS to determine who has added, deleted, or changed the data within AFMSS. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by AFMSS. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by AFMSS.

There is a risk that an application may be denied based on the submission of inaccurate information. All information is obtained directly from the applicant so is presumed to be complete and accurate. Any inaccurate information provided by the applicant may be corrected during APD review procedures.

There is a risk that individuals may not have clear notice due to the current System of Record status of review. BLM recognizes that INTERIOR/LLM-32, Land & Minerals Authorization Tracking System, 56 FR 5014 (February 7, 1991), modification published at 73 FR 17376 (April 1, 2008, and 86 FR 50156 (September 7, 2021) is currently being modified to incorporate four separate SORNs into one program area as described in Section 1.G. above. This consolidation effort is being completed to provide the most informative notice to the public about the existence and character of the land and minerals system of records maintained by BLM. The consolidated revision will update all sections of the notice to incorporate information pertaining to the consolidated system of records effort, to include a new routine uses and include simplified formatting of the previously published notice to reflect updates consistent with the DOI standard routine uses in accordance with the Office of Management and Budget (OMB) policy. These SORNS may be viewed at https://www.doi.gov/privacy. Individuals are also notified of the privacy practices through this PIA.

There is a risk that information may be maintained longer than necessary. This risk is mitigated by maintaining the records in accordance with the NARA-approved records schedules. The AFMSS records strictly follow BLM Records Control Schedules identified in Section 3.D. above in this PIA. Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA Guidelines.

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:

The use of the data is relevant and necessary since the PII in AFMSS is used to contact key personnel involved in the Oil & Gas operations to make arrangements for access, communicate inspection and enforcement findings, and to provide multiple types of notifications.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not Applicable. This system does not derive new data or create previously available data about an individual through data aggregation

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ 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

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

Only authorized BLM employees have access to all AFMSS data. There are some restrictions based on user's roles. Operators have restricted access only to their permit information and records.

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

Contractors are involved with the design/development and maintenance of AFMSS. All contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. 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 published procedures. The following Privacy Act contract clause was included in the contract:

"The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. Applicable Department of the Interior regulations concerning the Privacy Act are set forth in 43 CFR 2, subpart K. The CFR is available for public inspection at the Departmental Library, Main Interior Bldg., 1849 C St. NW, Washington DC, at each of the regional offices of bureaus of the Department and at many public libraries."

In addition, the Privacy Act clause 52.224-2 is referenced in the contract and those clauses can be viewed at 52.224-2 Privacy Act. | Acquisition.GOV.

☐ 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

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes

The System Security and Privacy Plan describes the practice of audit trails. System audit trails can identify and locate users by User ID and IP address and monitor individual users by

maintaining a record of activity and user activity including invalid logon attempts and access to data. All access is controlled by authentication methods to validate the authorized user.

☐ No

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

The audit logs record the username, IP address, timestamp, files accessed, and user action performed. Audit logs are maintained for seven years.

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

Only approved AFMSS administrators have the role/permission set to view this activity. The system implements all applicable security controls as defined by the NIST SP 800-53. Audit records are maintained, System Administrator actions are documented, and reports of activity are reviewed weekly by the system security staff. AFMSS follows the principal of least privilege so that only the least amount of access is given to a user to complete their required activity. BLM employees and contractors are required to complete annual security and privacy awareness training, and those employees authorized to manage, use, or operate a system are required to take additional Role Based Security and Privacy Training. All employees are required to sign annually, the DOI Rules of Behavior acknowledging their security and privacy responsibilities.

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

(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

(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

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 Assistant Director for Energy, Minerals, and Realty Management (HQ-300) is the Automated Fluid Minerals Support System (AFMSS) System Owner and the official responsible for oversight and management of the AFMSS security controls and the protection of agency information processed and stored in the AFMSS application. The Information System Owner and AFMSS Privacy Act System Manager, in collaboration with the DOI Senior Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the AFMSS application. These officials, DOI bureau and office emergency response officials, and authorized AFMSS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the AFMSS. They are also responsible for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments as well as, processing complaints in consultation with the BLM Associate Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The AFMSS System Owner and the Information Ssystem Security Officer are responsible for oversight and management of the AFMSS security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, authorized access, or disclosure of agency PII

is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established DOI procedures.