



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: November 9, 2021

Point of Contact:

Name: Catherine Brean

Title: BLM Associate Privacy Officer

Email: blm_wo_privacy@blm.gov

Phone: 830-225-3459

Address: BLM, IRM, DOI National Operations Center, Bldg. 50, Denver, Colorado 80224

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 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) facilitates the collection,



management and sharing of authorized use regulatory fluid mineral permits/reports and field operations inspection/enforcement data across Federal onshore operations including Indian Trust Lands. AFMSS core data includes permits, agreements, wells, production, approvals of operations bond and surety information, and operator compliance.

AFMSS is an enterprise application used to track oil and gas information on public and Indian land. It contains data concerning lease and agreement ownership, well identification, location, and history, including casing information, geologic formations, resource protection, production, and operator compliance. The system has an electronic commerce module to interface with the oil and gas industry.

- Application for Permit to Drill/Notices of Staking (APD/NOS) Module
- Automated Inspection & Enforcement (I&E) modules
- Internal and external Data Reporting
- Geothermal Resources Automated Support System (GRASS)
- Well Information System (WIS): Sundry and Well Completion Report Module

The personally identifiable information, PII, stored in AFMSS is the name and contact information for the private surface owner. The PII is collected to ensure the surface owner has been contacted by the oil and gas operator. 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.

The Operators (Oil and Gas Companies) are required to supply an email 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?

Bureau of Land Management, Minerals Management (43 CFR 3000) Alaska National Interest Land Conservation (16 U.S.C. 3101 et seq.)
Minerals Lands and Mining (30 U.S.C. 181 et seq., 301-306, 351-359, and 601 et seq.)
Money and Finance, Miscellaneous (31 U.S.C. 9701)
Public Buildings, Property and Works (40 U.S.C. 471 et seq.)
National Petroleum Reserve in Alaska (42 U.S.C. 6508)
Federal Land and Policy Management (43 U.S.C. 1701 et seq.)
Omnibus Budget Reconciliation Act of 1981 (Pub. L. 97-35 and 95 Stat. 357)

D. Why is this PIA being completed or modified?

- New Information System
- New Electronic Collection



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

E. Is this information system registered in CSAM?

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

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 <i>If Yes, provide a description.</i>
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 on 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: *Describe*

BLM 3160-3, 3160-4, and 3160-5 forms used to gather information for AFMSS have obtained OMB approval. The OMB Control Number is 1004-0137, title “Onshore Oil and Gas Operations and Production (43 CFR Parts 3160 and 3170).” The Expiration Date is November 30, 2021.



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
- Other: Specify the PII collected. Tribe Name, Application Permit to Drill (APD) number, Indian Mineral Lease Allottee, Lease Name, if applicable. (Note: this data can be searched in the system and associated PII data can be retrieved by a data relationship).

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 surface owner PII currently maintained in AFMSS is provided to BLM by third party Operators who have entered into agreements with individual surface owners. BLM employees or Operator(s) input the information into AFMSS from what is provided on the application which is used to verify an existing agreement is in place between Operator(s) and individual surface owners. The individual surface owners do not access the AFMSS system or submit their PII directly to BLM but do so, through a separate agreement with the Operator(s).

C. How will the information be collected? Indicate all that apply.

- Paper Format
- Email
- Face-to-Face Contact
- Web site
- Fax
- Telephone Interview
- Information Shared Between Systems *Describe*
- Other: *Describe*



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

The PII stored in AFMSS is the name and email address of the employee or agent of an Operator submitting Application Permit to Drill, Sundry Notices, and Well Completion Reports.

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 an Operator's name and email address associated with the account and can send email correspondence outside AFMSS to the user.
- Other Bureaus/Offices: 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: *Describe the Tribal, state or local agencies and how the data will be used.*
- Contractor: There are BLM contractors who provide development, operations and maintenance support to the AFMSS application.
- 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.*

An agreement is established between the Operator and the private surface owner as 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.

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.*

The BLM 3160-3, 3160-4, and 3160-5 forms contain a Privacy Act statement that has been furnished in connection with this application process.

Privacy Notice: *Describe each applicable format.*

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. The surface owner PII currently maintained in AFMSS is provided to BLM by third party Operators who have entered into agreements with individual surface owners. BLM employees or Operator(s) input the information into AFMSS from what is provided on the application which is used to verify an existing agreement is in place between Operator(s) and individual surface owners. The individual surface owners do not access the AFMSS system or submit their PII directly to BLM but do so, through a separate agreement with the Operator(s).

Other: *Describe each applicable format.*

The website where the operator logs in, external BLM Application Security System 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 and the well association is used to retrieve Indian Mineral lease allottee.

I. Will reports be produced on individuals?

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



No

Section 3. Attributes of System Data

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

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. The Indian Mineral lease allottee data is not checked for accuracy.

B. How will data be checked for completeness?

The AFMSS system requires that users provide their name and an email address to create an account. Initial login information is sent to the email address prior to the user first login into the system.

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

BLM field office users and management are responsible for reviewing the data for currency, completeness, accuracy, and updates throughout the well lifecycle. During the BLM adjudication, engineering, surface, and geological review processes, if there was a problem with the data, the BLM field office user would notify the Operator. The Operator would be responsible for making updates within the AFMSS system. AFMSS has a data validation mechanism to ensure data corresponds to proper formatting, for example, an email must have "name" "@ "domain-name.com" for the form to submit.

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

The AFMSS records are permanent, and the disposition authority states to "transfer a copy along with a public use version to NARA immediately, in accordance with NARA transfer instructions applicable at the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession." Data is indefinitely stored in AFMSS. Records maintained in AFMSS are covered by BLM records retention schedule 4/34



under disposition authority DAA-0049-2013-0004-0001, which was approved the National Archives and Records Administration (NARA).

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

The AFMSS records are permanent, and the disposition authority states to “transfer a copy along with a public use version to NARA immediately, in accordance with NARA transfer instructions applicable at the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession.”

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 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. 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 due for an update and the System Manager is currently revising the SORN to consolidate under one program area. The consolidated revision will update all sections of the existing notice and identify the consolidated system of records effort, in which 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); and 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) will be consolidated into the current SORN. It will also include new routine uses and 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.

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, as it provides BLM with surface owner contact information used to validate that a respective operator has or has not made an agreement for access. BLM uses Operator data to create an AFMSS account which allows Operator(s) to apply for permits and submit Sundry Notices and Well Completion Reports.

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. 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. *Describe the controls that are in place to protect the data from unauthorized access or use.*

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

No, data or processes are not being consolidated.

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

Users

Contractors

Developers

System Administrator

Other: *Describe*

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

Only authorized BLM employees have access to 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. There are technical contractors who have access to AFMSS and provide development, operations, and maintenance support to the system. The Privacy Act clause 52.224-2 is referenced in the contract.

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 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. *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 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 is 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, unauthorized 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.