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: Applicant Violator System (AVS)
Bureau/Office: Office of Surface Mining Reclamation and Enforcement (OSMRE)
Date: August 3, 2023
Point of Contact
Name: Patrick Dege
Title: Associate Privacy Officer
Email: osmre_privacy@osmre.gov
Phone: 202-208-3549
Address: 1849 C Street NW, 1200W, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Office of Surface Mining, Reclamation and Enforcement (OSMRE), Applicant/Violator System (AVS), is a relational database that implements section 510 (c) of the Surface Mining Control and Reclamation Act of 1977 (SMCRA). SMCRA specifies that no coal mining permits may be issued to applicants that have outstanding responsibilities for unabated mining violations.

The AVS delivers ownership, control, organizational, and violation data on a national basis to the 24 State Mining Regulatory Authorities, Tribes, and OSMRE staff who are responsible for determining permit eligibility. It is also used by the public as a source of public information about the mining industry. It provides a single point of inquiry for mining ownership, control, and violation information to assist the Regulatory Authorities (RA)'s in determining the eligibility of applicants for coal mining permits. The AVS is a mission critical program within OSMRE.

The AVS is an automated information system of applicant, permittee, operator, violation and related data that is maintained by OSMRE to assist in implementing the Surface Mining Control Reclamation Act (SMCRA). The AVS was established in 1987 to assist Federal and State permitting authorities with determining permit eligibility for surface coal mining by tracking applicants or their associated entities for unabated or uncorrected violations. The database serves as a Web-accessible reference source for regulatory and permitting authorities as well as the public. Since 1990, OSMRE has also used AVS to assist in implementing additional sections of the SMCRA, including sections 201, 506, 507, 510, 511, and 521.

AVS access is tiered based on user credentials. The general public or any interested party can log into the AVS as a guest, but guests cannot modify data and some fields may not be viewable. State and Tribal level users are provided training and given elevated privileges that allow them to modify data but there are controls such as they can only create and modify information and violations within their assigned State or Tribal area. The OSMRE staff that maintain the AVS database are given the highest level of access to modify data in order to assist all internal and external customers with database maintenance and create accounts for credentialed users.

C. What is the legal authority?

- The Surface Mining Control and Reclamation Act of 1977 (30 U.S.C. §§ 1201–1328)
- Code of Federal Regulations; Title 30, Chapter VII; Subchapter G, Parts 774, 778; Subchapter R, Part 874.
- The Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521) requires federal agencies to minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information.
- Government Organization and Employees, Departmental Regulations (5 U.S.C. 301)
- Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)
- E-Government Act of 2002 (Public Law 107-347)
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- Civil Action No. 81-2134, SAVE OUR CUMBERLAND MOUNTAINS, INC., et al., Plaintiffs, v. WILLIAM P. CLARK, et al., January 31, 1985.

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 DOI's Governance, Risk, and Compliance platform?

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

UII Code: 010-000000711 24-08-01-03-02-00 / OSM AVS-WIN SSPP

☐ 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: *List Privacy Act SORN Identifier(s)*

The AVS was under a prior System of Records Notice (SORN) that was rescinded in 1995. During this PIA review it was determined that a new SORN analysis is required to determine if re-establishment of a SORN is needed.

☐ No

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

☒ Yes:

Some types of entity information are collected and maintained using the "30 CFR 874.16 – Contractor Eligibility and the Abandoned Mine Land Contractor Information Form", OMB Control #: 1029-0119, Expiration Date: 2/28/2025 also known as the "ABANDONED MINE LANDS (AML) CONTRACTOR INFORMATION FORM"

Additional information included may be found under OMB Control #: 1029-0117, "30 CFR Part 778 - Permit Applications - minimum requirements for legal, financial, compliance, and related information" collection.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Employment Information
☒ Mailing/Home Address
☒ Other: Specify the PII collected.

A Tax ID Number or TIN is requested, and smaller coal company/entities or sole proprietors have been known to use their personal Social Security number in lieu of an Employer Identification Number. The applicant's name, application or permit number and associated Mine Safety Health Administration number, permit status, violation status, and violation number is included as part of the applicant record. Credentialed users' PII required to create and manage user accounts includes name, username, password, security questions and answers, organization affiliation, and work email address.

AVS includes information on all permanent program permit applicants and permittees and the identity of all persons who own or control such applicants or permittees as set forth in 30 USC 1257. The identity of all entities, including corporations, partnerships, and individuals, which are responsible for unabated cessation orders issued by OSMRE during the interim or permanent programs. The identity of all persons who own or control such entities. The identity of all entities which have failed to pay any penalty imposed by OSMRE under 30 USC. § 1268(h) in either the interim or permanent programs; and the identity of all persons who own or control such entities.

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*

Updates can be gathered from corporate sources, resident agents, or other authorized sources.

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*

Violation and/or entity information may be gathered from OSMRE's Inspection & Enforcement (I & E) system and the Coal Fee Collection Management System (CFCMS). There is no connection to AVS, and information is manually entered into the AVS by OSMRE AVS personnel.

☐ Other: *Describe*

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

PII is collected to determine applicant eligibility to receive a SMCRA permit to mine coal in the U.S.A. The AVS assists Federal and State permitting authorities in determining permit eligibility for surface coal mining by tracking applicants or their associated entities for unabated or uncorrected violations. The database serves as a Web-accessible reference source for regulatory and permitting authorities as well as the public.

The entered data is utilized to create accounts for credentialed OSMRE, State, and Tribal users. The users provide their work address, work phone number, and work email to establish their accounts.

Data is also collected per governing regulations to create ownership and control information of applicants for coal permits and AML Contracts. This ownership and control information involves disclosing the information required in 30 CFR 778.11 such as name, address, and phone numbers for individual officers as well as corporate parents. This information is used to establish an entity record in the AVS and to help prevent the creation of duplicate entities.

Ownership and control information is collected to create an Organizational Family Tree (OFT), that indicates what businesses and individuals control how mining and reclamation are conducted. To determine eligibility for a new permitting action or AML Contract, the entities in the OFT for an applicant are compared with the entities associated with uncorrected violations in

the AVS. Generally, if there are matches and the applicant is associated with violations, they are not eligible for a new permitting action or AML Contract.

The regulations at 30 CFR 778.11 also specify the collection of Tax ID for applicants and operators, however, a Tax ID is not required to create an entity. Tax IDs are also used to ensure a duplicate is not created when creating new business entities as some businesses have identical or similar names. Tax IDs are only viewable to credentialed OSMRE and State and tribe users.

After a permit is issued, if a violation is written on that permit and it remains uncorrected, the unabated violation will be entered into AVS, and the violation assigned to the individuals and businesses in the OFT of the permit. In this way the AVS acts as an enforcement tool with the goal of entities correcting their outstanding compliance issues to receive new permitting actions.

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.*

A limited number of OSMRE AVS Office staff can view and alter information provided by credentialed users in order to create or maintain their user accounts. AVS Office staff may export data from the system to be used to complete routine services for customers, report metrics, and conduct data quality reviews.

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

AVS data is sometimes used for research by DOI solicitors in cases of coal related bankruptcies and other investigations.

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

AVS data is sometimes used for research by Department of Justice in cases of coal related bankruptcies and other investigations. OSMRE does not have documented evidence of other federal agencies routinely utilizing the AVS but because public access to AVS is available it may be possible that other agencies are also using the system for research using the Guest view.

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

State and tribal entities that maintain primacy over their coal mining program generally have AVS users that receive training and credentialed AVS accounts. These users can view and modify data (with certain limits based on their state or tribal association). They can view information that is not viewable as a Guest such as Tax ID within their area of purview.

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

Government contractors that work for OSMRE may access and utilize AVS data to complete their work assignments.

IT Contractors hired by OSMRE to maintain the AVS hosting environment, and improve the database and application, have access to AVS data in order to complete their work.

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

Access by the public is available via Guest Log In, but the system does not display some types of data under this view such as Tax ID.

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.*

If a person, business, or entity wants to mine coal in the U.S., they must submit the information required at 30 CFR 778.11. If they don't submit this information, they are not eligible to receive a permit and are thus not eligible to mine coal in the U.S.

To receive an AVS account, State, tribal, and Federal users must complete an account form that contains some PII information. If they have concerns about privacy or use, they can address them to the AVS Office or their immediate supervisor who must also sign the account form.

☐ 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 Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment (PIA).

When accessing the AVS Application, the System Use Notification will be modified to contain a privacy notice for guest users. All credentialed users will be required to consent to the System Use Notification and privacy notice in order to access the AVS Application. Users who do not consent to the System Use Notification along with the privacy notice will not be able to access the system.

A privacy notice will be added to the "Abandoned Mine Lands (AML) Contractor Information Form" and the "AVS User Account Form"

☐ Other: *Describe each applicable format.*

☐ None

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

Common identifiers and search criteria are name, entity number, application or permit number, and violation number. Once a record is searched for and selected, the application can generate reports for users such as an OFT report which lists the individuals and businesses related to a specified entity and an eligibility evaluation which indicates if a selected record and their related entities are associated with any violations. These types of reports are available to all users including non-credentialed Guest users.

I. Will reports be produced on individuals?

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

In the system you can view and export ownership and control information that a specific individual is associated with such as all their current and former business relationships and officer roles in the coal mining sector. You can also generate an evaluation report for an individual which shows if that individual is associated with any violations. Any user including non-credentialed Guest users can generate these reports. The reports are used for research and to update or maintain State and federal permitting information and are considered public information.

☐ No

Section 3. Attributes of System Data

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

User account data is collected on "AVS User Account Form" which is signed by the employee's supervisor. The individuals applying for accounts are usually referred by an existing user or contact whose identity is already verified. The user's government email addresses are used to submit the account form and so we are certain they are from a legitimate source.

When creating and updating ownership and control information provided in the OSMRE-76 form, or via individual state and tribes, the data must fall into one of the following categories to be considered accurate and legitimate:

1. Submitted by an AVS Regulatory Authority contact who received it as part of the permit application or AML contracting process
2. Submitted by the company seeking to be updated and signed by an officer on the Organizational Family Tree
3. Submitted by an authorized person with a valid secretary certificate signed by an officer on the Organizational Family Tree

B. How will data be checked for completeness?

The system maintains some automated validation controls where records cannot be saved without essential data. Additionally, users receive training concerning data management best practices and standards which inform what should be considered "complete".

Whenever data quality reviews or other routine tasks indicate a record may not be complete or accurate in the AVS User Account Form, the OSMRE-76 form, or via individual state and tribes, the AVS Office staff follows up with the appropriate contact to attempt to resolve the issue.

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

It is on the burden of the corporate entities applying for permitting actions and AML Contracts to submit all information as required in 30 CFR 778 and changes to their ownership and control data within 60 days of the change (30 CFR 774.12). Regulators are charged to update the AVS within 30 days of receipt of the change (30 CFR 774.11).

In order to facilitate data quality, the AVS Office also completes a variety of data quality reviews including but not limited to:

- New entity check
- Entities with permits and no relationships
- Applications pending in the system more than a year
- Division of Financial Management and Division of Compliance Management reconciliation requests

User accounts are created and deactivated throughout the year as needed. They are also verified annually to ensure users are still using their accounts as assigned.

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

AVS records are maintained under OSMRE Records Schedule N1-471-10-001.

Master Data Files have a disposition of PERMANENT. Copies of the master data files are to be transferred to the National Archives at end of every 3rd fiscal year as specified in National Archives standards at time of transfer.

Reference Data Files have a disposition of TEMPORARY. Files should be reviewed annually and then destroy or delete when no longer needed for business use or reference need.

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

Approved disposition methods include shredding, burning, or pulping paper records, and degaussing or erasing electronic records in accordance with NARA guidelines and Departmental policy. However, data (electronic and paper) files transferred to the Federal Record Center (FRC) are disposed of via methods determined by the FRC.

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 to individuals that is mitigated by the security and privacy controls implemented to safeguard privacy and the limited collection of personally identifiable information (PII) from individuals. For credentialed users PII maintained in the system is constrained to name, username, password, organization affiliation, and work email address that are required to create and manage user accounts. For businesses and individuals listed in the ownership and control of an applicant for a coal mining permit or AML Contract PII maintained in the system is limited to name, address, phone number, employment information, Tax ID, and aliases. The protection and maintenance of information for recovery and backup purposes is done following OSMRE policy and process for backup and retention of information. System permissions and access controls are in place to limit system access to only those authorized individuals with the proper authorization to perform official functions.

Tax ID information is not viewable to public users. Credentialed users who can enter and update information can view stored Tax ID information for research purposes. Entity and permitting records used in implementing eligibility evaluations are permanently stored in the AVS as a historic record to demonstrate ownership and control over time unless there is a clearly documented situation where the record or associated information was created in the AVS erroneously.

There is nominal risk to the privacy of official user information throughout the information lifecycle. Risk is reduced by following established guidance from NIST SP 800-53 on access controls. Privacy risk to AVS System accounts would affect usernames, passwords and security questions and answers. These risks are mitigated by a combination of administrative, physical and technical controls. The AVS System has a Moderate system security categorization in accordance with NIST standards and Federal Information Processing Standard (FIPS) 199, and the Federal Information Security Modernization Act (FISMA).

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls. Risk is also mitigated

through system configuration controls that limit or prevent access to privacy information. The AVS System utilizes appropriate security and privacy controls implemented to safeguard information collection, use, retention, processing, disclosure, destruction, transmittal, storage, and audit logging. It covers access controls, password management, firewalls, segregation of duties, and encryption of database, media, and communications. The AVS System utilizes the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following NIST, FISMA, OSMRE, and DOI security and privacy policies. All access is controlled by authentication methods including multi-factor authentication (MFA). All DOI employees and contractors are required to complete annual security and privacy awareness training and sign DOI Rules of Behavior. OSMRE Personnel authorized to manage, use, or operate the AVS System application are required to take additional role-based privacy and security training annually. AVS System data is under the control of its system owner, the DOI regions 1 and 2 Program Assistance Division Chief, who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with OSMRE and DOI privacy officials.

There is a risk of unauthorized access, use or disclosure of the records in the system. These risks are mitigated by safeguards including access restrictions based on least privilege, use of username and password, role-based training, and other controls to ensure the confidentiality, integrity and availability of the records. The authorized personnel and system administrators' complete privacy, security, records, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information awareness training and privacy and security role-based training on an annual basis. Access to records in the system is limited to authorized personnel whose official duties require such access. Electronic data will be protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual's web browser will be encrypted using approved federal encryption protocols that meet National Institute of Standards and Technology (NIST) standards. These security measures will establish different degrees of access for different types of users. Ongoing system development will require MFA, at the point of entry as another security control to mitigate the risk of unauthorized access, use or disclosure of the records in the system.

Information may be shared with law enforcement organizations as necessary for any investigations related to a violation or entity involved in an investigation. However, appropriate safeguards such as encrypted media is utilized to ensure that PII is protected. A SORN is being considered for development and will provide additional routine uses for disclosures.

AVS contract provides continuous monitoring, vulnerability management, contingency planning, FISMA compliance, intrusion detection, incident response, and assessment and authorization (A&A).

The system is hosted in a certified FedRAMP cloud-based environment employing security and privacy controls defined by NIST Special Publication (SP) 800-53. The systems cloud-based

environment meets FedRAMP and FISMA compliance standards and per the FIPS 199 form review its categorization is Moderate.

There is a risk that users may not receive adequate notice of the purpose and uses of their information. This risk is mitigated by the privacy notice posted on the OSMRE AVS site and this PIA. Username and email address is collected directly from the individual and is used for the purpose of creating user accounts, authenticating users to the site, and access to the data contained within the AVS. Users voluntarily provide information in order to receive user accounts or apply for coal mining applications or AML Contracts.

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

There is a risk that records may be maintaining longer than authorized or necessary to meet a business need. Records are maintained in accordance with a NARA approved schedule. Once the retention period is deemed to be over, the records are destroyed in accordance with approved methods as outlined in DOI policy and the applicable records schedule.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The information is used to determine applicant eligibility to receive a SMCRA permit to mine coal in the U.S.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

N/A - The system does not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

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

Anyone who consents to the System Use Notification and privacy notice can access the Publicly accessible information as a guest user but has no ability to edit, modify, or change data. They also cannot view all information stored in the database, for example Tax ID information is not viewable to non-credentialed guest users.

Users with credentials receive elevated permissions to the AVS application which correspond to their work duties. As an example, State users are given accounts where the can create and modify permitting and violation records associated with their assigned state, but do not have privileges to create or modify these records for other states. OSMRE Auditors have access to some special reports but do not have the ability to modify any data. OSMRE AVS Staff are granted access to modify any data in the system in any state and create and manage user accounts.

A very limited number of OSMRE staff and the AVS hosting contractor staff have access to the backend of the AVS and can run queries, export data, and modify data through the backend if needed. These staff have received additional training and hourly backups of the AVS are maintained during business hours in case a catastrophic issue requires a restore to a previous version.

Electronic data will be protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual's web browser will be encrypted using approved federal encryption protocols. These security measures will establish different degrees of access for different types of users.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The appropriate Privacy Act contract clauses were included in the contract. Current contracts not in compliance with the Information Technology (IT) Baseline Compliance Contract Guidelines memorandum of August 15, 2022, will be modified to comply.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

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

☒ Yes. *Explanation*

The purpose of the OSMRE AVS is not to monitor individuals, however user actions and use of the system are logged in compliance with DOI security policies. Data captured include username, user's last date of login, date of user content creation, date user content was modified.

Additionally, the application tracks the IP that is access the application, user's login/logout and how long they are in the application.

When a registered user performs a system function, a record of that activity is created and is attributed to them. The system does not actively monitor portal users and is not programmed to do so.

☐ No

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

The system does not actively monitor portal users and is not programmed to do so. Audit logs are maintained in the system and track login attempts and errors. Audit logs record username, date/time, actions.

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

The applications governance plan outlines the roles and responsibilities of users with elevated access to the administration functions. The outline uses the principle of least privilege to provide only the level of access required to perform in their role. Audit logs capture user actions and use of the system, which are monitored to meet OSMRE and DOI security policies.

Privacy notices and continuous system monitoring notices will be posted prominently. The AVS contract provides continuous monitoring, vulnerability management, contingency planning, FISMA compliance, intrusion detection, and incident response.

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*

Physical controls are inherited from the cloud service provider, such as locked server rooms, cipher locks and controlled physical server access.

(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*

MFA is required from credentialed users and must be U.S. based to access the application.

(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*

Annual role-based security and privacy training is required for OSMRE credentialed users and administrators.

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 DOI Regions 1 and 2 Program Assistance Division Chief serves as the OSMRE AVS system owner and the official responsible for oversight and management of the OSMRE AVS system security controls and the protection of agency information processed and stored by the OSMRE AVS system. The Program Assistance Division Chief is also responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies, as well as processing complaints, in consultation with the OSMRE Associate Privacy Officer (APO).

The OSMRE AVS system owner is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including the reporting the loss, compromise, unauthorized disclosure, or access of individuals' personal information, in consultation with the OSMRE APO.

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

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

The OSMRE AVS system owner is responsible for oversight and management of the OSMRE AVS system security and privacy controls, and for ensuring to the greatest possible extent that the OSMRE AVS system is properly managed, and that access is granted in a secure and auditable manner.

The OSMRE AVS system owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the OSMRE APO and the OSMRE Incident Response Team in accordance with the DOI Privacy Breach Response Plan and the OSMRE Incident Response Plan.

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