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: Safety of Dams Environmental Monitoring System (SDEMS)
Bureau/Office: Bureau of Indian Affairs, Office of Trust Services, Division of Water and Power
Date: November 3, 2021

Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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?

It is the mission of the Division of Water and Power (DWP) to promote self-determination, economic opportunities, and public safety through the sound management of irrigation, dam, and power facilities owned by the Bureau of Indian Affairs (BIA). The BIA Safety of Dams (SOD) program was established under the Indian Dams Safety Act of 1994, Public Law No. 103-302 (25 U.S.C. § 3801 et seq.). Its mission is to reduce the potential loss of human life and property damage caused by dam failure by making BIA dams as safe as practically possible. It is responsible for all dams on Indian land. These dams form a significant part of water resources and trust assets for Indian reservations. Dam safety activities include but are not limited to: (1)

risk management and risk reduction; (2) emergency management, including Emergency Action Plans (EAPs) and Environmental Monitoring; (3) inspections and evaluations; (4) maintenance and repairs; and (5) security.

The BIA SOD Branch operates and maintains an environmental monitoring system that monitors and provides notifications on environmental conditions and equipment status at and near BIA SOD Program Dams. SDEMS is a commercial, off-the-shelf (COTS) minor system provided as Software-as-a-Service hosted on the Amazon Web Services, FedRAMP-certified cloud service. The system performs automated real-time data collection, processing, validation, analysis, archiving and visualization of hydro-meteorological and equipment sensor data and transmits the environmental monitoring data via satellite over a secure connection for use by the SOD Program. Notifications are sent to BIA or Tribal employees responsible for monitoring safety of dams on Tribal lands and not members of the public. It is important to note that this is not a Supervisory Control and Data Acquisition (SCADA) system, it does not control gates.

C. What is the legal authority?

Indian Dams Safety Act of 1994, Public Law No. 103-302 (25 U.S.C. § 3801 et seq.)

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*

☒ No: SDEMS is undergoing CSAM registration.

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.*
Contrail	Software that organizes data in a database and displays it on a website. It also manages notifications of environmental conditions monitored by the system.	Yes	Work-related information: names and work phone number and work emails.

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)*

☒ No

SDEMS is not a Privacy Act system of record. However, some records in SDEMS are maintained under DOI system of records notices, which may be viewed at https://www.doi.gov/privacy/sorn.

- DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, modification published 86 FR 50156 (September 7, 2021) for BIA login records to access the SDEMS system, and
- DOI-58, Employee Administrative Records, 75 FR 19384, April 20, 1999, modification published 86 FR 50156 (September 7, 2021) contact information for emergency contact purposes.

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

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

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

☒ Name

☒ Other: SDEMS collects the minimum information necessary to send notifications about environmental conditions monitored by the system. SDEMS users provide work-related contact information, such as official email address and official cell phone number. However, some individuals may provide their personal contact information at their discretion. Official cell phone numbers are collected only for those requesting text notifications from the system. Official emails from SOD safety personnel are collected for notifications and for user authentication, password reset.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

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

☐ Paper Format
☒ Email
☒ Face-to-Face Contact
☐ Web site
☐ Fax
☐ Telephone Interview

☐ Information Shared Between Systems
☐ Other: *Describe*

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

Names, work email addresses and cell phone numbers are used to manage system login and to send notifications of environmental conditions monitored by the system.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Information may be shared with BIA SOD system administrators acting in their official capacity to update User access and to send notifications of environmental conditions monitored by the system.

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

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

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

Information may be shared with Tribal Officials acting in their official capacity when needed to update or validate Tribal dam safety personnel access for notifications of environmental conditions monitored by the system.

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

Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support, and update User access and notifications of environmental conditions monitored by the system.

☐ 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.*

Individuals may verbally or in writing decline to provide their contact information (name, work email address, or cell phone number) for access to this system and to receive notifications of environmental conditions monitored by the system, which will result in these individuals not being granted access or receive notifications of dam environmental conditions.

☐ 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.*

SDEMS is not a Privacy Act system of record. Privacy notice is provided through publication of this privacy impact assessment and the published DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, modification published 86 FR 50158 (September 7, 2021) for login records to access the SDEMS system and DOI-58, Employee Administrative Records, 75 FR 19384, April 20, 1999, modification published 86 FR 50158 (September 7, 2021)contact information for emergency contact purposes. These SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other: *Describe each applicable format.*

☐ None

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

Administrative users with approved privileged access login to the system use manual processes to retrieve names, email addresses, and cell phone numbers to update automated notifications of environmental conditions monitored by the system and website user accounts.

I. Will reports be produced on individuals?

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

Reports are not produced on individuals. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit logs also collect information on system users such as username. System administrators and the information system owner have access to these activity reports. Audits are conducted on all administrative functions including privileged operations, data calibration updates, data edits, site/sensor additions and deletions, user account management.

☐ No

Section 3. Attributes of System Data

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

Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy and verified by the individual's supervisor before account creation. If for some reason information provided for text messages becomes inaccurate, an error message is sent back to the system.

B. How will data be checked for completeness?

Users are responsible for ensuring the completeness of the data associated with their user accounts. Data is checked for completeness by the individual's supervisor before account creation. If for some reason information provided for text messages becomes inaccurate, an error message is sent back to the system.

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

User account information is provided directly by the user for account creation. Data is checked for currency by the individual's supervisor before account creation. Supervisors as needed, submit updates to User account and notification information to the BIA Central Office Safety of Dams staff. The Regional Safety of Dams Officer and site supervisor periodically conduct information verification via email and phone calls.

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

Paper records are covered by Indian Affairs Records Schedule (IARS) Records Series 4900 – Irrigation and Power and have been scheduled as permanent records by the National Archives and Records Administration (NARA) under Job No. N1-075-04-006, approved November 21, 2003. Records may include Safety of Dams program and project files, emergency management program and project files, and maintenance program and project files. Records are maintained in the office of record for a maximum of 5 years. Records are cut-off at the end of the fiscal year. The records are then retired to the American Indian Records Repository which is a Federal Records Center. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the United States Department of the Interior (DOI) and NARA.

System usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), approved by NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

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

Data and information maintained within the BIA Environmental Monitoring System is retained under the appropriate NARA approved IARS. Disposition of data follow NARA guidelines and approved Records Schedule for transfer, pre-accession, and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIA's records retention schedule. System administrators dispose of DOI records by shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

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 low risk to the privacy of individuals due to the non-sensitive, work-related PII contained in SDEMS. SDEMS collects the minimum information necessary to send notifications of environmental conditions monitored by the system. SDEMS users provide work-related contact information. However, some individuals may provide their personal contact information at their discretion.

SDEMS has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. SDEMS is rated as a FISMA low system requiring management, operational, and technical controls established by NIST SP 800-53 to mitigate privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, or exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access are based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages SDEMS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of SDEMS user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Employees annually complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they understand their responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that SDEMS may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained to perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed

written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, for complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, based on the "least privilege" principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. SDEMS meets BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. This risk is mitigated through periodic reviews and validation of User account and information needed to make notifications of environmental conditions monitored by the system. User account information is provided directly by the user before account creation. Supervisors as needed, submit updates to User account and notification information to the BIA Central Office Safety of Dams staff. In addition, an email is periodically sent to system users requesting verification of their information, which is then confirmed with the site supervisor or Regional Safety of Dams Officer.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The Division of Water and Power is responsible for managing and disposing of BIA records in SDEMS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. Division of Water and Power ensures only records needed to support its program, Tribes, and Tribal members is maintained. Division of Water and Power maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-04-006: Series 4900 – Irrigation and Power. SDEMS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off. Information collected and stored within SDEMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published DOI-47, HSPD-12: Logical Security Files (Enterprise Access

Control Service/EACS), 72 FR 11040, March 12, 2007, modification published 86 FR 50156 (September 7, 2021) for login records to access the SDEMS system and DOI-58, Employee Administrative Records, 75 FR 19384, April 20, 1999, modification published 86 FR 50156 (September 7, 2021) contact information for emergency contact purposes, which may be viewed at: https://www.doi.gov/privacy/sorn. The PIA and applicable SORNs provide a detailed description of system source data elements and how an individual's PII is used.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. SDEMS is hosted and administered within a DOI-approved and FedRAMP-certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP certification. The data residing in the system is backed up on a nightly basis.

In addition to the risk mitigation actions described above, the BIA maintains an audit trail of activity is maintained sufficiently to reconstruct security relevant events. The BIA follows the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST SP 800-53. DOI employees must take Information Management Training (IMT) which includes Cybersecurity, Privacy, Records Management, and Controlled Unclassified Information (CUI) before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the 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.

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 use of the system and data collected is relevant and necessary to the purpose for which SDEMS was designed and supports the Indian Affairs Division of Water and Power mission to promote self-determination, economic opportunities, and public safety through the sound management of irrigation, dam, and power facilities owned by BIA. The BIA SOD program was established under the Indian Dams Safety Act of 1994, Public Law No. 103-302 (25 U.S.C. § 3801 et seq.).

☐ 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. SDEMS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

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

Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages SDEMS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of SDEMS user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

Users and non-administrator contractors only have access to environmental monitoring data and cannot access any names, email addresses, or phone numbers other than their own login information. The System Administrators have access to all data, including names, email addresses, and cell phone numbers.

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

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

Contractors 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. Contract modification prior to exercising first option year included: Revised FAR 52.212-5, to include by reference the following clauses, are included in the contract:

- 52.224-3, Privacy Act Training
- 52.239-1, Privacy or Security Safeguard (Aug 1996)

☐ 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 SDEMS is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system.

☐ No

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

The SDEMS system is not intended to monitor individuals; however, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

SDEMS can audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. SDEMS System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. SDEMS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to SDEMS Rules of Behavior. Users must complete annual IMT Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and CUI training before being granted access to the DOI network or any DOI system, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The SDEMS audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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. Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens. AWS employee and third-party access to the data center is only granted to approved employees. All individuals needing access must apply for access and provide a valid business justification. Access is granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

(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 Associate Chief Information Officer is the Information System Owner. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in SDEMS. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the DOI Privacy Officials.

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 SDEMS ISO and ISSO are responsible for the central oversight and management of the SDEMS security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The SDEMS ISO, ISSO, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within one hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.