U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Bison System Access Management
System or Project Acronym:	BASM
Bureau or Office:	OCIO
Date Signed:	July 6, 2026
System Operational Status:	Operational

Point of Contact

Name:	Constance Sue Sheffer
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☒ Significant Modification
☐ Other: Describe below

The FY 2026 BASM Privacy Threshold Analysis identified material changes to BASM functionality, integrations, identity records, lifecycle automation, PIV credential metadata, reporting capabilities, and data flows that were not fully represented in the prior 2018 privacy assessment. This PIA documents the current BASM functionality and privacy posture.

2. What is the purpose of the system or project?

Bison System Access Management is DOI's enterprise identity and access management application. BSAM consolidates identity, employment, directory, credential, training, and access related attributes received from

authoritative DOI systems to support identity lifecycle management across the Department.

BSAM uses SailPoint IdentityIQ to create consolidated identity records and support rule-based workflows for establishing, activating, modifying, reviewing, disabling, and deprovisioning user accounts and access. The system also provides authorized reporting, search, access certification, compliance monitoring, and operational dashboards.

BSAM receives information from DOI Access, DOI Talent, and DOI.NET/Active Directory. It provides approved identity or system activity information to authorized DOI systems, including the DOI Emergency Notification System, Bison Support System, Main Interior Building Physical Access Control System, Splunk, and Axonius.

BSAM receives selected PIV credential metadata from DOI Access. DOI Access is part of the USAccess program and is designated as a High Value Asset based on its availability requirements. BSAM is not itself designated as a High Value Asset.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

BSAM is registered in BisonGRC under UII: 010-000002258.

4. What legal authorities authorize the collection and use of data in this system or project?

BASM maintains and uses identity, credential, account, training-status, and access information to administer authorized access to DOI information systems and facilities and to support Department-wide identity and access management.

Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, establishes Government-wide requirements for secure and reliable identification of Federal employees and contractors and supports DOI identity, credential, and logical-access functions.

Federal Information Processing Standard (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors, establishes the Federal PIV requirements used to implement HSPD-12.

Other Federal and DOI authorities applicable to workforce administration, information-system operation, and access management support the underlying identity and account-management functions performed through BASM.

The Privacy Act of 1974, Federal Information Security Modernization Act, E-Government Act, OMB Circular A-130, NIST security and privacy standards, and applicable DOI policies establish requirements governing how BASM information is assessed, secured, maintained, used, disclosed, and managed throughout its lifecycle..

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

BSAM retrieves and reports records using individual-linked identifiers, including name, username, account ID, Applicant ID, work email address, certificate or credential identifiers, and other identity attributes. Privacy Act System of Records Notice coverage is therefore required.

The primary Privacy Act System of Records Notice (SORN) governing BSAM's consolidated identity and access management records is:

INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS).

To the extent BSAM receives and maintains copies of information originating in other authoritative systems, the source records may also be subject to:

GSA/GOVT-7, HSPD-12 USAccess, 80 FR 64416 (October 23, 2015), for PIV identity proofing, enrollment, credential issuance, and related USAccess records; and
INTERIOR/DOI-16, Learning Management System, 83 FR 50682 (October 9, 2018), for training and certification records maintained in DOI Talent.

DOI-47 is the principal SORN for BSAM's consolidated logical access and identity management records. The other SORNs govern applicable source-system records and do not replace DOI-47 for BSAM's own retrieval and use of identity and access records.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

BSAM does not collect information directly from members of the public through a form, survey, questionnaire, or other public-facing collection. It receives workforce identity and access information from existing DOI authoritative systems. Therefore, BSAM does not conduct an information collection requiring approval under the Paperwork Reduction Act.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None.

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)	☐ Home telephone number	☒ Employment or resume info
☐ Aliases/nickname	☐ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☐ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics/facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information

☐ Sex	☐ Marital status	☐ Passport information
☐ Race or ethnicity	☐ Spouse Information	☐ Travel information
☐ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☐ Emergency contact info	☐ Credit card number
☐ Personal cell phone number	☐ Financial information	☐ Nationality
☒ Username / user ID / acct ID	☐ IP address / network ID	☐ Device ID / online ID
☐ Geolocation / GPS / location	☐ Photos / video / audio	☐ Health / medical information
☐ Tribal or other ID number	☐ Education information	☐ Disability Information
☐ Criminal / disciplinary info	☐ Military records	☒ Other: Describe below

BASM maintains identity, employment or affiliation, directory, credential, training-status, account, access, workflow, and audit information necessary to perform enterprise identity and access management.

Information includes name, DOI work email address, username and account identifiers, Applicant ID, bureau or office, job title, duty station or office location, employment or affiliation status, supervisor relationship, account status, group memberships, roles and entitlements, training or certification status, selected PIV credential metadata, certificate identifiers, lifecycle workflow information, and user-linked application and audit information.

Application and security logs may also contain network, system, certificate, or device-related identifiers associated with authorized BASM activity.

BASM does not maintain Social Security numbers, personal contact information, financial information, health information, or biometric templates.

2. What is the source for the PII collected? Check all that apply.

☐ Individual	☒ DOI Records
☐ Federal Agency	☐ Third Party Records
☐ Tribal Agency	☐ State Agency
☐ Local Agency	☐ Other: *Describe Below*

BSAM receives PII from DOI authoritative systems, primarily DOI Access, DOI Talent, and DOI.NET/Active Directory. These systems provide the identity, employment or affiliation, credential, directory, training, certification, and access attributes used to create and maintain consolidated BSAM identity records.

BSAM does not collect identity information directly from individuals and does not obtain identity records from commercial, State, local, tribal, or other non-DOI sources

3. How will the information be collected? Check all that apply.

☐ Paper Format	☐ Fax
☐ Email	☐ Telephone Interview
☐ Face-to-Face Contact	☒ Shared Between Systems: *Describe*
☐ Website	☐ Other: *Describe*

Information is collected through automated, authenticated system-to-system interfaces and scheduled data

exchanges with DOI Access, DOI Talent, and DOI.NET/Active Directory. BSAM also generates application and audit records during normal operation.

BSAM does not collect PII through paper forms, fax, email, telephone interviews, face-to-face collection, or a public-facing website.

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

BSAM uses PII to support DOI enterprise identity and access management. The information is used to:

- Create and maintain consolidated identity records;
- Establish, activate, modify, review, disable, and deprovision accounts and access;
- Apply predefined identity lifecycle and access-management rules;
- Support access certification and periodic access reviews;
- Confirm employment, affiliation, credential, account, and training status;
- Provide authorized reporting, search, operational dashboards, and compliance monitoring;
- Supply approved identity attributes to connected DOI systems for emergency notifications, service support, physical access, and other authorized DOI operations;
- Maintain application and audit logs;
- Detect, investigate, and respond to unauthorized access, account misuse, or other security incidents; and
- Support DOI cybersecurity, privacy, records, audit, and accountability requirements.

BSAM information is not used for commercial purposes, public profiling, or AI-based scoring.

5. How does this project limit the collection and use of PII to only what is necessary?

BSAM limits collection to identity, credential, directory, training, account, access, and logging attributes required to perform approved identity and access management functions. Data elements are received from designated DOI authoritative systems rather than collected independently or duplicated through separate manual collection processes.

Access to BSAM data is restricted through role-based access controls, least-privilege permissions, need-to-know determinations, PIV or multi-factor authentication, and periodic access review. Reports and dashboards are limited to attributes necessary for the approved operational purpose, and bulk export capabilities are restricted to authorized personnel. Administrative activity and access to identity information are logged and monitored.

The BSAM program reviews data feeds, reports, roles, and integrations when system functions change to identify and remove attributes or access that are no longer required.

Section 3: Data Sharing and Individual Rights

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

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.

☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☐ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☐ **Other Third-Party Sources:** Describe how the data will be used below.

Within OCIO: Authorized Identity and Access Management personnel, system administrators, developers, security personnel, privacy personnel, auditors, and program officials may access BSAM information when required to administer the system, manage identities and access, conduct access reviews, investigate account or security issues, and perform compliance and oversight responsibilities.

Other DOI bureaus and offices: Authorized bureau or office IAM representatives, supervisors, security personnel, and program officials may receive or access identity and access information necessary to request, approve, review, certify, modify, or terminate access and investigate unauthorized or inappropriate activity.

BSAM exchanges identity and access information with authorized DOI enterprise systems to support identity lifecycle management, access provisioning, security monitoring, emergency notification, physical access management, and operational support. Each interface exchanges only the information necessary to perform its authorized business function and is protected through role-based access controls, least privilege, and applicable DOI security and privacy requirements.

BSAM exchanges information with the following authorized DOI systems:
Inbound Interfaces (information received by BSAM):

- DOI Access: Receives identity, employment or affiliation status, supervisor information, and selected PIV/CAC credential metadata.
- DOI Talent: Receives name, username, DOI work email, manager information, and training or certification compliance status.
- DOI.NET/Active Directory: Receives directory, account, certificate, group membership, and related access attributes.

Outbound Interfaces (information provided by BSAM):

- DOI Emergency Notification System: Provides approved identity attributes needed to establish or maintain workforce emergency-notification records.
- Bison Support System: Provides identity attributes needed for authorized service management, user support, and system operations.
- Main Interior Building Physical Access Control System: Provides limited identity and employment status information needed to administer authorized physical access.
- Splunk: Receives BSAM application, audit, and security event information to support centralized logging, monitoring, security analysis, alerting, auditing and incident response.
- Axonius: Receives approved identity and asset-related information to support enterprise asset management, correlation, compliance monitoring, and cybersecurity operations.

Contractors: Authorized contractors supporting BSAM design, development, operation, or maintenance may access information only when necessary to perform assigned duties. Contractor access is subject to background investigation or credentialing, Rules of Behavior, required privacy and security training, role-based access, least privilege, audit logging, and applicable contract privacy and security clauses.

BSAM does not routinely share PII with non-DOI Federal, State, local, tribal, commercial, or other third-party organizations. Any disclosure outside DOI would be made only when legally authorized and consistent with the

Privacy Act and applicable SORN routine uses.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

BASM does not currently rely on an external MOU, MOA, or ISA for the routine information exchanges described in this PIA because those exchanges occur among DOI systems.

BASM's internal system-to-system connections are documented and governed through applicable DOI system authorization, interface, security, and operational documentation.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals cannot decline the maintenance and use of the identity and access attributes required to establish, authenticate, manage, monitor, review, and terminate access to DOI systems and facilities. BSAM does not collect this information directly from individuals; it receives required workforce identity and access information from authoritative DOI systems.

DOI employees, contractors, and associates are informed of applicable identity, credential, access, and monitoring requirements through source-system notices, applicable Privacy Act Statements where information is originally collected, published SORNs and PIAs, DOI Rules of Behavior, required privacy and security training, and system login banners.

Use of DOI information systems is conditioned on compliance with DOI access and monitoring requirements. A user may decline to use DOI computing resources, but cannot opt out of identity management, authentication, access control, audit logging, or security monitoring while maintaining authorized DOI system access.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☒ Privacy Act Statement:
☒ Privacy Notice:
☒ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

BSAM generally does not collect information directly from individuals. Notice is provided at the point of original collection by the authoritative source systems through applicable Privacy Act Statements and privacy notices.

Additional notice is provided through this PIA and applicable SORNs, including DOI-47 for logical access and

identity management records, GSA/GOVT-7 for applicable USAccess/PIV records, and DOI-16 for applicable DOI Talent training records.

DOI employees, contractors, and associates are also informed through DOI Rules of Behavior, initial and annual privacy and security training, and system login banners. The login banner advises users that DOI systems and activity may be monitored for authorized purposes and that users should not expect privacy when using Government information systems.

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

BSAM records may be retrieved, searched, filtered, or reported by name; username; user ID or account ID; Applicant ID; DOI work email address; bureau or office; duty station or physical office location; employment, affiliation, account, access, PIV, training, or certification status; supervisor or manager relationship; group membership; assigned role or entitlement; certificate identifier; and other Active Directory, credential, or identity attributes.

Application and audit records may also be retrieved by username or account identifier, administrative role, event type, system action, date and time, or other system generated identifier."

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

BSAM produces reports and dashboards containing information associated with individuals. These may include name, username, account ID, Applicant ID, DOI work email address, bureau or office, duty station, employment or affiliation status, account and access status, group memberships, assigned roles, credential status, training or certification compliance, supervisor relationships, and related identity attributes.

Reports support identity lifecycle management, access provisioning and deprovisioning, access certification, compliance monitoring, account administration, auditing, troubleshooting, and authorized investigations of access-related or security issues.

Access is limited to authorized IAM personnel, system administrators, security and compliance personnel, designated bureau IAM representatives, auditors, and other officials with a valid need to know. Access is controlled through role-based permissions, least privilege, PIV or multi-factor authentication, logging, monitoring, and periodic access reviews. Report export and bulk access are restricted based on assigned role and approved business need.

Reports may include information received through the authorized system interfaces described above and are limited to users with an approved business need.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

BASM contains multiple record categories that may be subject to different NARA-approved disposition authorities. These include consolidated identity records, account and access-management records, PIV/certificate metadata, training-status information, application and audit logs, reports and exports, information transmitted to enterprise monitoring systems, and backup records.

The OCIO Records Officer is validating the applicable NARA-approved disposition authority, item, retention period, and disposition trigger for each BASM record category.

Until applicable disposition authority is confirmed, BASM Federal records will be preserved and will not be destroyed based solely on system configuration, business-use determinations, or automated deletion settings.

This section will be updated with the validated disposition authorities and retention requirements before final implementation of automated disposition.

2. What measures are used to maintain the accuracy and completeness of data received from external sources after receipt and throughout the records lifecycle?

☐ External-source data is received and validated as described below
☒ N/A: The system does not receive data from sources other than DOI records

BSAM does not receive PII from non-DOI sources. Data is received from authoritative DOI systems through automated interfaces and scheduled synchronization processes.

BSAM uses interface validation, required-field checks, reconciliation processes, exception reporting, and operational review to identify missing, incomplete, duplicate, or inconsistent records. Identity and access management personnel may also compare BSAM information with the applicable authoritative source when resolving an account, access, credential, training, or employment-status issue.

BSAM does not independently alter authoritative employment, credential, directory, or training information. Errors are referred to the responsible source system or program office for correction and are incorporated into BSAM through subsequent synchronization.

Corrections are made in the applicable authoritative source system and are reflected in BSAM through scheduled synchronization processes.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

BSAM maintains application and audit logs that record authentication events, identity record access, searches, reporting activity, lifecycle workflow actions, record updates, access changes, administrative actions, and other security-relevant events, as applicable.

Logs identify the user or administrative account associated with the activity and record relevant event details such as date, time, action performed, affected account or object, and outcome. BSAM log information is provided to Splunk and Axonius for centralized monitoring, alerting, correlation, security analysis, asset correlation, auditing, and incident response.

Access to logs is restricted to authorized IAM, system administration, cybersecurity, audit, and incident response personnel with a need to know. Log activity is reviewed for anomalous behavior, unauthorized access attempts, excessive or inappropriate use, and other potential policies or security violations.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

I Collection and aggregation risk: BSAM consolidates identity, credential, directory, training, account, access, and location-related information from multiple DOI systems. Consolidation increases the potential impact of unauthorized access and creates a risk that inaccurate or unnecessary attributes may be imported.

Mitigation: BSAM receives information only from designated DOI authoritative sources and limits collection to attributes required for approved identity and access management functions. Automated interfaces, validation, reconciliation, exception handling, and source-system correction processes reduce the risk of incomplete or inaccurate records. Data feeds and required attributes are reviewed when integrations or business requirements change.

Use and access risk: Authorized users could view, search, report, export, or use identity information beyond what is necessary for their assigned duties. Reports and dashboards may make aggregated information more readily accessible.

Mitigation: Access is limited by role-based access controls, least privilege, need-to-know determinations, PIV or multi-factor authentication, separation of duties, formal access approval, periodic access reviews, logging, monitoring, and restrictions on bulk export. Users complete required privacy, security, records, and Rules of Behavior training.

Accuracy and lifecycle-automation risk: Inaccurate employment, supervisor, credential, training, account, or access information could result in an account being established, changed, retained, disabled, or deprovisioned incorrectly.

Mitigation: BSAM relies on designated authoritative sources, applies predefined rules rather than AI-based inference, records workflow actions, and permits review and correction through the responsible source system and IAM support processes. Access certifications and periodic reviews provide additional validation.

Disclosure and integration risk: Information transmitted to connected DOI systems could be disclosed to unauthorized recipients, used beyond the approved purpose, or include more attributes than the receiving system requires.

Mitigation: Internal data exchanges are limited to approved DOI systems and documented operational purposes. System-to-system connections are authenticated and protected in transit. Data elements are limited to those needed by the receiving function, and access is restricted to authorized personnel. Disclosures outside DOI are not routine and may occur only when legally authorized and consistent with applicable SORN routine uses.

Logging and monitoring risk: Audit logs may reveal information about an individual's system access, account activity, administrative actions, or association with a security investigation.

Mitigation: Log access is restricted to authorized personnel, logging data is used only for approved security, auditing, troubleshooting, and accountability purposes, and activity is monitored through enterprise security tools.

Retention risk: Retaining identity, account, access, or log records longer than necessary increases the period during which information could be misused or exposed.

Mitigation: Records will be mapped to specific NARA-approved schedules and disposed of when the authorized retention period expires. Until the records review and automated disposition capabilities are completed, records remain subject to restricted access, encryption, monitoring, and other approved safeguards.

Incident risk: Unauthorized access, compromise, or exfiltration could expose identity, credential, employment, access, or system activity information.

Mitigation: BSAM uses encryption, network protections, role-based access, PIV or MFA authentication, audit logging, centralized monitoring, incident detection, and DOI incident response procedures. Suspected or confirmed incidents are reported to DOI-CIRC and appropriate privacy officials.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

BASM creates new identity and access-management information through rule-based lifecycle processing. The system combines authoritative identity, employment or affiliation, credential, training-status, directory, account, and access information and applies predefined business rules to generate workflow actions, account and access status changes, certification actions, notifications, and audit records.

BASM does not generate predictive scores, rankings, behavioral profiles, or AI-based inferences about individuals. Its automated processing is based on predefined identity and access-management rules and authoritative source data.

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

☐ Yes: *Provide explanation below*
☒ No

BASM records lifecycle and access-management actions associated with an individual's identity record, including

workflow status, account and access changes, certification activity, and related administrative or audit information. These records document actions taken through the identity and access-management process.

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

☐ Yes: *Provide explanation below*
☒ No

BASM applies predefined business rules to authoritative source information to determine and execute identity and access-management actions, such as establishing, modifying, disabling, or deprovisioning an account or access entitlement.

These are rule-based access-management determinations rather than AI-based, predictive, or discretionary assessments. The underlying source information remains subject to validation through the authoritative source system, and access-management actions are logged and subject to applicable review, certification, exception handling, and administrative oversight.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

BASM relies on designated authoritative DOI source systems for the identity, employment, credential, directory, training, and access attributes used by lifecycle workflows. Automated actions are governed by documented business rules and are subject to reconciliation, exception handling, access certification, audit logging, and administrative review. Errors in authoritative attributes are referred to the responsible source system for correction and are reflected in BASM through subsequent synchronization.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☐ Yes
☒ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

N/A. BASM does not use AI or machine learning models.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☐ No

N/A. BASM does not make AI-based decisions affecting individuals.

4. Are safeguards in place to prevent bias or unintended consequences?

☐ Yes
☐ No

N/A. BASM does not use AI or machine learning models that introduce AI-specific bias or model-related consequences.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☐ Yes
☐ No

N/A. BASM does not use AI or machine learning models requiring model review or retraining.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☐ No

N/A. BASM does not use federated learning or conduct AI or machine learning model training.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

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

Access to BSAM is limited to authorized IAM staff, system administrators, developers, contractors supporting BSAM operations, designated bureau IAM representatives, security and compliance personnel, auditors, and other officials with an approved business need.

Access is requested and approved through formal account and access-management procedures and is assigned according to job responsibilities, need to know, least privilege, separation of duties, and role-based permissions. Administrative and privileged access requires DOI network access and PIV or multi-factor authentication.

Users are limited to the data and functions required for their assigned role. Access is periodically reviewed and recertified, and access is modified or removed when duties change or the individual no longer requires access. Authentication, searches, reports, data changes, workflow actions, administrative actions, and other security-relevant activity are logged and monitored.

2. What data protection policies apply to cloud-based PII storage?

Not applicable. BSAM is hosted in an on-premises environment and does not store PII in a cloud environment. Therefore, cloud specific data protection policies do not apply. PII is protected through the administrative,

technical, and physical safeguards implemented for the on premises environment in accordance with DOI security policies, the approved System Security and Privacy Plan (SSPP), and applicable NIST security and privacy controls..

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

BSAM uses application, authentication, and audit logs to record identity record access, searches, reports, updates, workflow actions, administrative actions, access changes, and other security-relevant activity. Log information is forwarded to Splunk and Axonius for centralized monitoring, alerting, event correlation, asset correlation, security analysis, and incident response.

DOI cybersecurity and authorized BSAM personnel monitor for unsuccessful authentication, anomalous account activity, inappropriate privilege use, unusual report or export activity, unauthorized access attempts, unexpected changes, and other indicators of misuse or exfiltration.

Monitoring is supported by role-based access controls, least privilege, separation of duties, restricted privileged accounts, PIV or multi-factor authentication, encryption, firewalls, network controls, periodic access review, and DOI incident response procedures.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

BSAM monitors activity associated with the use and administration of the system through application, authentication, and audit logging. Audit records may identify the individual user or service account that accessed a record, performed a search, generated a report, modified an identity or access attribute, initiated or approved a workflow, or performed another authorized administrative action.

Monitoring is conducted solely to support identity and access management, system security, auditing, troubleshooting, compliance, and incident response. BSAM is not used for unrelated surveillance or employee performance evaluation.

Access to monitoring information is restricted to authorized identity and access management personnel, system administrators, cybersecurity personnel, auditors, and incident response personnel with a demonstrated need to know. Appropriate use of this capability is enforced through role-based access controls, least privilege, Personal Identity Verification (PIV)-based or other multi-factor authentication, Rules of Behavior, required privacy and security training, audit logging, periodic access reviews, supervisory oversight, and applicable DOI policy.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors participate in BSAM design, development, operation, and maintenance as authorized under their contracts and assigned duties. Contractors must meet applicable DOI personnel security and credentialing requirements; sign DOI Rules of Behavior and any required nondisclosure agreements; complete initial and annual privacy, security, records, and role-based training; and comply with BSAM access control, logging, monitoring, incident reporting, and data-handling requirements.

Contractor access is limited by role, need to know, and least privilege and is reviewed and removed when no longer required. Applicable contracts must include required Privacy Act, privacy training, and information security clauses when contractor personnel operate a system of records or have access to Privacy Act records.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☐ Other: *Describe Below*

Describe the other types of controls implemented.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

PIV/MFA, role-based access, least privilege, audit logging, centralized monitoring, restricted export.

Administrative Controls

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Other: *Describe Below*
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

Periodic access recertification, separation of duties, incident response procedures.

BSAM protects PII through layered physical, technical, and administrative controls consistent with the system's SSPP and authorization requirements.

Physical access to facilities and infrastructure is restricted to authorized individuals through controlled facilities,

identification badges, guards or facility security personnel, electronic access controls, and surveillance where applicable.

Technical controls include PIV or multi-factor authentication, unique user identification, role-based access, least privilege, separation of duties, firewalls, network protections, encryption in transit and at rest, VPN or protected remote access, PKI certificates, audit logging, centralized monitoring through Splunk and Axonius, and restrictions on privileged access and bulk export.

Administrative controls include formal access approval, periodic access recertification, security and privacy assessments, Rules of Behavior, mandatory privacy, security, records, and role-based training, contractor requirements, incident response procedures, system monitoring, and removal of access when it is no longer required

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals may file a privacy complaint concerning BSAM to the DOI Departmental Privacy Office through the DOI Privacy Program contact channels or the Department's privacy support request process.

Written correspondence may be directed to:

Departmental Privacy Office
U.S. Department of the Interior
1849 C Street NW
Washington, DC 20240

Complaints are reviewed and tracked by the appropriate DOI privacy officials and may be coordinated with the BSAM System Owner, Information System Security Officer, cybersecurity officials, records officials, legal counsel, or other responsible offices. DOI evaluates the matter, determines whether corrective action is required, documents the disposition, and responds to the complainant as appropriate.
Current electronic contact and submission information is available through the DOI Privacy Program website.

8. What processes are in place for individuals to access their information?

Individuals seeking access to records about themselves may submit a written request under the Privacy Act of 1974 and DOI's Privacy Act regulations. Requests should identify the applicable system of records, describe the records sought, and include sufficient information to locate the records.

Requests must include the requester's full name, current address or other contact information, a description of the records requested, the approximate dates or circumstances associated with the records, and any other information required by the applicable SORN. The request must be signed, and identity must be verified in accordance with DOI Privacy Act procedures, such as through a notarized statement, an unsworn declaration under penalty of perjury, or another approved identity-verification method.

Requests may be directed to the system manager or Privacy Act contact identified in the applicable SORN or submitted through DOI's established FOIA/Privacy Act request channels. DOI will verify identity before disclosing records and will provide records through an appropriately secure method.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may request amendment of records about themselves under 5 U.S.C. § 552a(d) and DOI's Privacy Act regulations. A request should identify the record to be corrected, describe the requested correction, explain why the existing information is inaccurate, incomplete, untimely, or irrelevant, and include supporting documentation when available.

The request must be signed, and the requester's identity must be verified using the same procedures applicable to Privacy Act access requests. Requests may be submitted to the system manager or Privacy Act contact identified in the applicable SORN or through DOI's established Privacy Act request channels.

Because BSAM receives many attributes from authoritative DOI source systems, an identified error may need to be corrected first in DOI Access, DOI Talent, DOI.NET/Active Directory, or another responsible source system. Once corrected at the authoritative source, the updated information will be incorporated into BSAM through the applicable synchronization process.

DOI documents the request and determination and provides the requester with written notice of the outcome and applicable appeal right.

10. 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 BSAM System Owner is responsible for operational oversight, proper use of BSAM data, implementation of approved privacy and security controls, and ensuring that access is authorized, limited, reviewed, and auditable.

The Information System Security Officer supports security control implementation, monitoring, assessment, incident coordination, and system authorization responsibilities. IAM managers, system administrators, developers, contractors, and other authorized users are responsible for using information only for approved purposes and reporting suspected loss, compromise, unauthorized access, misuse, or disclosure.

Suspected or confirmed incidents involving PII must be reported immediately through DOI's established incident reporting process to DOI-CIRC and appropriate privacy and management officials in accordance with DOI policy. The Departmental Privacy Office evaluates privacy risk, coordinates required response and notification activities, and supports mitigation and corrective action

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

Suspected or confirmed loss, compromise, unauthorized access, misuse, or disclosure of BSAM PII will be reported immediately through DOI's established incident reporting procedures to DOI-CIRC and appropriate privacy, security, and management officials.

The BSAM System Owner, ISSO, system administrators, and cybersecurity personnel will take immediate action to contain the incident, prevent further unauthorized access or disclosure, preserve relevant evidence and logs,

and protect affected systems and records.

DOI-CIRC, the Departmental Privacy Office, the BSAM program, and other appropriate officials will assess the nature and scope of the incident, the PII involved, the individuals affected, the likelihood and potential severity of harm, whether information was acquired or viewed, and the safeguards already in place.

Based on the incident assessment and applicable Federal and DOI requirements, DOI will determine whether affected individuals, law enforcement, oversight entities, or other organizations must be notified. Any individual notice will describe the incident, the information involved, steps DOI has taken, actions individuals may take to reduce harm, and available points of contact or assistance.

BSAM will support remediation by correcting control weaknesses, modifying access, preserving and reviewing logs, improving monitoring, updating procedures or training, and documenting lessons learned and corrective actions.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed at least annually as part of DOI privacy and FISMA review activities and whenever a change could affect BSAM's privacy risk posture. An updated PTA and, when required, an updated or amended PIA will be completed before or in connection with material changes to system functions, technologies, hosting, data elements, sources, retrieval methods, integrations, sharing, reporting or analytics, automated processing, user populations, retention, or security and privacy controls.