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: Beneficiary Contact Management System (BCMS)
Bureau/Office: Bureau of Trust Funds Administration, Field Operations
Date: April 16, 2024
Point of Contact
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: btfa_privacy@btfa.gov
Phone: 505-219-7641
Address: 4400 Masthead St. NE, Albuquerque, New Mexico 87109

Section 1. General System Information

A. Is a full PIA required?

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

☐ No:

B. What is the purpose of the system?

The Bureau of Trust Funds Administration (BTFA), Beneficiary Contact Management System (BCMS), is a Customer Relationship Management (CRM) system that assists BTFA in meeting the fiduciary responsibilities set forth in the American Indian Trust Fund Management Reform Act of 1994. BTFA has fiduciary responsibilities including management of the receipt,

investment, disbursement, and administration of money held in trust for individual Indians and Alaskan Natives (or their heirs), and Indian tribes, and ensures timely, accurate, and consistent responses to beneficiary inquiries.

BCMS is used to manage and track all beneficiary contacts/interactions related to their Individual Indian Money (IIM) accounts, Tribal Trust accounts, Indian Trust land, and other revenue sources. The system pulls beneficiary information from BTFA's Single Source of Truth (SSoT) which includes data from BTFA's Trust Fund Accounting System (TFAS), Innovest. See Innovest PIA at https://www.doi.gov/sites/doi.gov/files/uploads/tfas-innovest-pia.pdf for an assessment of the privacy risks. BCMS pushes data to other BTFA applications including the One-Time (1x) Disbursement application, Debit Card application, and the Single Account Modification System (SAMS). BTFA's Amazon Connect Cloud Call Center (ACCCC) integrates with the BCMS to allow a beneficiary to leverage ACCCC integrated voice response technology for self-service (e.g., existing BCMS case status, beneficiary account balance and last disbursement). The integration securely passes encrypted user input with verification from ACCCC to BCMS to return a data response.

The Software as a Service (SaaS) is a FedRAMP authorized solution containing data rated as Federal Information Security Modernization Act (FISMA) Moderate according to its National Institute of Standards and Technology (NIST) FIPS-199 evaluation. The SaaS instance is in the Salesforce Government Cloud Plus which maintains a FedRAMP High authorization. Access is restricted to authorized BTFA employees, Bureau of Indian Affairs (BIA) employees, and contractors. Authorized users authenticate using their PIV card and OpenID Connect (OIDC), leveraging the Department of the Interior (DOI) Active Directory Federation Services (ADFS) with Azure Active Directory (AD).

C. What is the legal authority?

The American Indian Trust Fund Management Reform Act of 1994 (Pub. L. 103–412, 108 Stat. 4239); 25 U.S.C. 42, American Indian Trust Fund Management Reform; 25 U.S.C. 116, 117(a)(b)(c), 118, 119, 120, 121, 151, 159, 161(a), 162(a); 4011, 4043(b)(2)(B); Pub. L. 93-638, Self-Governance Compacts; 25 U.S.C. 5363(d)(1); 25 CFR 1000.350; 25 CFR 1000.355; 25 CFR 1000.365; and OMB Circular A-130, Managing Information as a Strategic Resource.

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 the Governance, Risk, and Compliance platform?

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

UII Code: 010-000002512; Beneficiary Contact Management System (BCMS) Security and Privacy Plan.

☐ No

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

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

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

☒ Yes:

Records maintained in the BCMS are covered by INTERIOR/OS-02, Individual Indian Money (IIM) Trust Funds, 84 FR 44321 (August 23, 2019). This SORN may be viewed at https://doi.gov/privacy/os-notices. This notice is currently being amended to reflect the reorganization of the BTFA and general updates.

☐ No

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

☒ Yes:

Office of Management and Budget (OMB) Control #1035-0004, Trust Funds for tribes and individual Indians, 25 CFR Part 115; Expiration date: 04/30/2024. The form is used within BTFA as, BTFA-01-004, Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address. The form is being renewed.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Other Names Used
☒ Truncated SSN
☒ Place of Birth
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Mailing/Home Address
☒ Other:

Beneficiaries' financial institution routing and account numbers, date of death if applicable, tribal affiliation, blood quantum, and contact information for individuals who may know the whereabouts of beneficiaries whose location is unknown.

BTFA has fiduciary responsibilities including management of the receipt, investment, disbursement, and administration of money held in trust for individual Indians and Alaskan Natives (or their heirs), and Indian tribes, and ensures timely, accurate, and consistent responses to beneficiary inquiries. BTFA requires beneficiary identification verification procedures that require the beneficiary to correctly answer four of six security questions (e.g., full SSN, date of birth, address, tribal enrollment number or tribal affiliation, date and amount of last check received, mother's maiden name).

SSN is used pursuant to 31 U.S.C. 7701 to manage trust fund accounts for individual (beneficiary) account holders to obtain or retain a benefit of individual Indian Money account by authority of the American Indian Trust Funds Management Reform Act of 1994.

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:

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: BCMS retrieves beneficiary data from BTFA's SSoT database which includes beneficiary information stored in BTFA's TFAS, Innovest. BTFA's ACCCC integrates with the BCMS to allow a beneficiary to leverage ACCCC integrated voice response technology for self-service (e.g., existing BCMS case status, beneficiary account balance and last disbursement). The integration securely passes encrypted user input with verification from ACCCC to BCMS to return a data response.

☐ Other:

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

BTFA performs trust responsibilities on behalf of the Secretary of the Interior. Certain data elements, including personally identifiable information (PII), are a necessary part of doing business and are not used for other than required or authorized purposes. Trust account holders are required to provide PII to obtain the benefit of having an IIM account on the BTFA-01-004 form, Trust Funds for tribes and Individual Indians, 25 CFR Part 115, OMB Control #1035-0004, Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address, Expiration date 01/31/2024. The form is being renewed.

The intended use of PII is to manage the receipt, investment, distribution, and disbursement of

IIM account and tribal trust fund income; provide trust services and information for Indian trust funds program management; manage beneficiary contact including inquiries and requests regarding their trust assets; provide IIM account status to IIM account holders; and locate IIM account holders whose whereabouts are currently unknown.

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

☒ Within the Bureau/Office: PII is shared with authorized BTFA employees acting in their official capacity. The data allows authorized BTFA users to perform essential functions for trust account holders. PII may be shared externally pursuant to the authorized routine uses identified in the INTERIOR/OS-02, IIM Trust Funds, 84 FR 44321 (August 23, 2019), SORN which may be viewed at: https://www.doi.gov/privacy/sorn. This notice is currently being amended to reflect the reorganization of the BTFA and general updates.

☒ Other Bureaus/Offices: PII is shared with authorized BIA employees acting in their official capacity. The data allows authorized BIA users to perform essential functions (e.g., social services, probate) for trust account holders.

☒ Other Federal Agencies: PII may be shared with the Department of the Treasury to report on payments, taxes and disburse funds, the Department of Justice as necessary to perform essential functions, and other agencies for official purposes in support of the system pursuant to the authorized routine uses identified in the INTERIOR/OS-02, Individual Indian Money (IIM) Trust Funds, 84 FR 44321 (August 23, 2019), SORN which may be viewed at: https://doi.gov/privacy/os-notices. This notice is currently being amended.

☒ Tribal, State or Local Agencies: PII is shared with authorized employees of tribes that have contracted or compacted the IIM trust funds program with access to the BCMS data, through Public Law 93-638. Compacted program trust funds program refers to an executed document that affirms the government-to-government relationship between a self-governance tribe and the United States. A self-governance compact is an executed document that affirms the government-to-government relationship between a self-governance tribe and the United States. The 1975 Indian Self-Determination and Education Assistance Act, Public Law 93-638, gave Indian tribes the authority to contract with the Federal government to operate programs serving their tribal members and other eligible persons. The amendment to the Act, entitled the 1994 Tribal Self-Governance Act, was added to allow tribes to compact federal government program services and functions.

☒ Contractor: Contractors have access to BCMS to perform services requiring access to these records on DOI's behalf to carry out the purpose of the system.

☐ Other Third Party Sources:

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

☒ Yes:

Trust account holders provide PII to obtain the benefit of having an IIM account on the BTFA-01-004 form (Trust Funds for Tribes and Individual Indians, 25 CFR Part 115, OMB Control # 1035-0004, Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address form, Expiration date 01/31/2024). This form is currently being renewed. Respondents voluntarily provide information to gain or retain a benefit, such as access to trust account funds held in trust.

☐ No:

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

☒ Privacy Act Statement:

A Privacy Act Statement is provided to individuals on the OMB Control #1035-0004, BTFA-01-004, IIM Instructions for Disbursement of Funds and Change of Address form, or over the telephone when they call the Trust Beneficiary Call Center (TBCC) or BTFA Field Offices.

☒ Privacy Notice:

Notice is also provided to individuals through the publication of this privacy impact assessment and the INTERIOR/OS-02, IIM Trust Funds, SORN which may be viewed at: https://www.doi.gov/privacy/os-notices. This notice is currently being amended to reflect the reorganization of the BTFA and general updates.

☒ Other:

Individuals who call TBCC are informed that calls may be monitored and recorded for quality assurance and training purposes. The DOI security banner alerts all authorized users of the system and DOI network that they are subject to monitoring and have no expectation of privacy.

☐ None

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

Records can be retrieved using the beneficiary's name, SSN, IIM or tribal trust fund account number(s), tribal affiliation, telephone number, mailing address, and system case number. Information is retrieved by trained individuals with authorized access to BCMS in the

performance of official functions. Users with the proper permissions can create customized result sets containing any information in the system.

I. Will reports be produced on individuals?

☒ Yes:

Reports generated internally are used for tracking beneficiary interactions and managing IIM and tribal trust accounts. Reports can be generated to determine how many times a beneficiary or tribe requests information related to their respective account and the type of interaction. Reports may be used by authorized staff within BTFA. Reports may include account information about IIM account holder, if SSNs are used it is for authorized purposes as authorized by 31 U.S.C. 7701.

An audit trail of activity will be maintained sufficiently to reconstruct security relevant events. The audit trail includes the identity of user's 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 are reported to BTFA IT Security.

☐ No

Section 3. Attributes of System Data

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

Data collected directly from individuals is presumed to be accurate at the time of submission and individuals can update their information at any time to ensure it remains accurate. Data received from other BTFA systems is presumed to be accurate at the time of retrieval. The data is verified for accuracy by the submitting entity and through updates or amendments, as needed, by authorized BTFA users. Authorized users are responsible for verifying data based on their access level and job duties.

B. How will data be checked for completeness?

Data collected directly from individuals is presumed to be accurate and complete at the time of submission. Quality assurance (QA) processes are in place and data is checked for completeness by the individual account holder and the system itself. It is also the responsibility of the authorized users entering the data into the system to check for completeness of the data. Authorized users are responsible for ensuring the information is accurate, correct, and current by verifying the information.

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

Individuals can update their information at any time to ensure it remains current. Steps to ensure data is current are in the Handbook for the Management of Trust Beneficiary Contacts. Data is entered and updated on a regular basis.

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

The National Archives and Records Administration (NARA) approved retention schedule for BTFA is the Indian Affairs Records Schedule (IARS). BCMS records are scheduled in the IARS as TR-6174-TBCC and approved as permanent data files (NARA Job #N1-075-07-7, TBCC). Records retention periods may be suspended by litigation holds, court orders, preservation notices, and similar by the Office of the Solicitor, BTFA Records Officer, and/or other authorized officials.

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 BCMS are retained under the appropriate NARA IARS. Data disposition follows the NARA guidelines and approved records schedule for transfer, pre-accession, and accession activities to NARA. These activities will also comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and Departmental and BTFA Records Management policies and procedures.

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 risk to individual privacy due to the type and volume of sensitive PII maintained by the system related to the individual's name, address, phone number, date of birth, date of death, SSN, Tribal affiliation, financial documents, account number(s), and other categories of records associated with financial and investment activity. Risks may include lack of adequate notice, maintaining inaccurate data, collecting more data or retaining records longer than necessary, unauthorized access, unauthorized disclosure, and misuse of data in the system. These risks are mitigated through a variety of operational, administrative, physical, technical, and privacy and security controls to protect the confidentiality, integrity, and availability of the information.

User access is granted only to authorized individuals by system administrators, and users are granted access only to data needed to perform their job duties. Only authorized users are provided access to BCMS using single sign-on and validated through the DOI ADFS and Azure AD. Administrative access to BCMS is granted only to authorized personnel on an official need to know basis. Unique administrator identification and authentication, least privileges and audit

logs are utilized to ensure appropriate permission and access levels. All user access policies and procedures are documented and reviewed regularly for necessary updates.

All users of DOI network resources, including contractors, must consent to DOI Rules of Behavior and take annual end-user security, privacy awareness, and records training to obtain access to any DOI network resource. BCMS administrators are also required to take security and privacy role-based training.

There is a risk that PII maintained in the system may be inaccurate. The data is checked for accuracy when requested from the beneficiary for identity verification or as information is submitted by the beneficiary. Individuals may update their information to ensure it remains accurate, complete, and current.

There is a risk that individuals may not have adequate notice regarding the collection of their information or the purposes for how the information will be used. Individuals are notified of the purpose of collecting information through the INTERIOR/OS-02, IIM Trust Funds, SORN, and this privacy impact assessment (PIA). Individuals are also provided a Privacy Act statement on the BTFA-01-004 form. There is an automated message informing individuals who call the TBCC that calls may be monitored and recorded for quality assurance and training purposes. A DOI security banner alerts all authorized users of the system and DOI network that they are subject to monitoring and have no expectation of privacy.

There is a risk that more information may be collected than is necessary. This risk is mitigated by only using the minimal amount of information necessary to effectively meet the requirements for validating information prior to initiating IIM account changes. In addition, access is restricted to only authorized users that are allowed to access the system with a "need-to-know" to perform their official duties.

There is a risk that unauthorized individuals could potentially gain access to the PII, may be used for an unauthorized purpose, or PII is collected and stored on a cloud system. These risks are mitigated by implementing security and privacy controls to protect the data, including technical controls to restrict and manage access and granting access to authorized personnel based on the least privilege principle to perform official duties. The SaaS is FISMA Moderate authorized and rated as a FISMA Moderate system with controls implemented to protect data in accordance with Federal laws, policy and standards. Electronic data is protected through user identification, passwords, system permissions and software controls, and different access levels are established for different types of users. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training, including role-based security and/or privacy training and sign the BTFA Rules of Behavior before authorized to access the system. The use of BTFA/DOI IT systems is conducted in accordance with the appropriate BTFA/DOI use policy. All access is controlled by authentication methods to validate the authorized user.

An audit trail of activity will be maintained sufficiently to reconstruct security relevant events. The audit trail includes the identity of user's 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 are reported to BTFA IT Security. BTFA 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 multi-factor authentication. Users are granted authorized access to perform their official duties and such privileges must comply with the principles of separation of duties. Controls over information privacy and security are compliant with the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

There is a risk that information in BCMS may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored is limited to the minimal amount of data needed to meet BTFA's mission and business functions. Records are maintained in accordance with records retention schedules that are approved by NARA and as permanent due to their fiduciary and historical value for the administration of money held in trust for individual Indians and Alaskan Natives. Users are also reminded through policy and training that they must follow the applicable retentions schedules and requirements of the Federal Records Act. The data in BCMS are closely safeguarded in accordance with applicable laws, rules, and policies.

There is a risk that PII may be exposed by authorized users or disclosed to unauthorized users. This risk is mitigated by ensuring that proper safeguards are in place in accordance with 43 CFR 2.226. Computerized records containing sensitive PII are protected by following the NIST standards that comply with the Privacy Act of 1974 (as amended), Paperwork Reduction Act, FISMA of 2014, and the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. Data is protected through user identification, passwords, system permissions, and software controls. System security measures establish different access controls for different types of users associated with pre-defined groups and/or bureaus. It is possible that an authorized BCMS user has PII visible on their computer display and a passerby could see the data. To mitigate the risk, BCMS users are instructed to safeguard their computer and lock their screen when stepping away from their workstation.

User access is restricted to only the functions and data necessary to perform their duties based on specific functions and is restricted using role-based access. Authorized personnel and contractors sign a network rules of behavior form, are trained and required to follow established internal security protocols, and must complete annual Federal Information Systems Security Awareness, Privacy and Records Management training courses. Contract employees are monitored by their Contracting Officer Representative (COR) and the Associate Chief Information Security Officer (ACISO).

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:

BCMS data allows BTFA to perform essential functions for trust beneficiaries and tribes, including managing and tracking all beneficiary contacts/interactions related to their IIM accounts, tribal trust accounts, Indian trust land, and other revenue sources.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not Applicable. The system does not derive new data. Data collected directly from individuals is presumed to be accurate at the time of submission, data is verified by the submitting entity and through updates or amendments to ensure data is accurate, correct, and current. Authorized users are responsible for verifying data based on their access level and job duties.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

Access to data is limited to those authorized users that have a need to know in order to perform official duties, including System Administrator(s), authorized program personnel, and contractors based on least privileges.

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

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒Other: Users, Contractors, Developers, and System Administrators are given access to BCMS data on a 'least privilege' basis and a 'need-to-know' to perform official functions. Contractors and developers supporting the system and performing system maintenance and other related activities may have access to the data in the system.

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

All authorized BTFA users have access to view account information. Access is limited to authorized personnel who have a need to access the data in the performance of their official duties; electronic data is protected through user identification, passwords, system permissions and software controls; security measures establish different access levels for different types of users associated with pre-defined groups and/or bureaus; each user's access is restricted to only the functions and data necessary to perform their job; access can be restricted to specific functions. Authorized users are trained and required to follow established internal security protocols, must complete all security, privacy, and records management training, and sign the BTFA Rules of Behavior. Contract employees with authorized access to the system are monitored by the COR and ACISO. The Information System Owner, system manager, and supervisors determine user access based on the role and duties of the employee (contractor). Access to all data is restricted to authorized personnel based on official need-to-know.

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.

The appropriate Privacy Act, security, other contract clauses and privacy terms and conditions are inserted in their contract.

☐ No

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

☐ Yes.

☒ No

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

☒ Yes.

Audit records are maintained that identify when account asset, name/address information is created, maintained/changed, and deleted. System logs capture date and time users log in and any changes that are initiated.

☐ No

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

The BCMS is not intended to monitor individuals. Audit logs can be used to run reports detailing an individual users' authorized access and actions performed in the BCMS. Information collected as a function of monitoring authorized user's may include username, failed attempts, files accessed, and user actions. Audit logs are reviewed on a regular, periodic basis, and any suspected attempts of unauthorized access or scanning of the system are reported to BTFA IT Security.

Authorized users are trained and required to follow established internal security protocols, must complete all security, privacy, and records management training, and sign the BTFA Rules of Behavior. Contract employees with access to the system are monitored by the COR and ACISO.

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

Access to BCMS is limited to authorized personnel who have a need to access the data in the performance of their official duties; electronic data is protected through user identification, passwords, database permissions, and software controls; security measures establish different access levels for different types of users associated with pre-defined groups and/or bureaus; each user's access is restricted to only the functions and data necessary to perform their job; access can be restricted to specific functions (create, update, delete, view, assign permissions) and is restricted utilizing role-based access. An audit trail of activity will be maintained sufficient to reconstruct security relevant events. Audit logging is utilized to assess security posture in the identification of potential incidents or compromised systems. The system performs account monitoring by maintaining a consistent and accurate monitoring process of account and data access.

Authorized users are trained and required to follow established internal security protocols, must complete all security, privacy, and records management training, and sign the DOI Rules of Behavior. Contract employees with access to the system are monitored by the COR and ACISO.

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:* The BCMS agents may be virtual, teleworking or at one of the DOI offices and required to safeguard government-furnished equipment and are required to protect privacy data.

(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*

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view. In addition, firewalls and network security arrangement are built into the architecture of the system and NIST guidelines and Departmental policies are implemented for system and data security. System Administrators monitor the activities of authorized users to ensure that the BCMS is properly used.

Additionally, the audit trail features identification, authentication and password requirements, and mandatory security, privacy, and records management training requirements prevents unauthorized access to data, browsing, and misuse.

All personnel must consent to DOI Rules of Behavior and complete annual mandatory security, privacy, and records management training in order to received and maintain access to the DOI network or systems.

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 Deputy Bureau Director, Trust Operations – Field, as the Information System Owner (ISO), and the System Administrator are responsible for oversight, management, and protection of trust account information processed and stored by the BCMS.

The ISO, Information System Security Officer (ISSO), Privacy Act System Manager, and data owners are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data maintained and stored in BCMS and accessed by authorized BTFA and contractor employees. They are also responsible for protecting the privacy rights of the employees and customers for the information collected, maintained and used in BCMS. The System Manager and data owners are responsible for meeting the requirements of the Privacy Act, providing adequate notice, making determinations on Privacy Act requests, for notification, access, amendments, and complaints in consultation with the BTFA Associate Privacy Officer (APO).

The ISO and cloud service provider(s) are also responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies and for protecting the privacy rights of the public.

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 ISO, ISSO, and System Administrator(s) are responsible for ensuring use of BCMS. Authorized users are also responsible for ensuring the proper use of BCMS in accordance with Federal Laws and policies. The ISO and ISSO and all authorized users are responsible for protecting individual privacy and reporting any potential compromise to the APO in accordance with Federal policy and established DOI/BTFA procedures. The BTFA APO and the ISSO coordinate the investigation of reported violations from users. They are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.