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: Box Index Search System (BISS)
Bureau/Office: Bureau of Trust Funds Administration (BTFA)
Date: February 3, 2021
Point of Contact:
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: btfa_privacy@btfa.gov
Phone: (505) 816-1615
Address: 4400 Masthead Street N.E., Albuquerque, NM 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 Box Index Search System (BISS), allows the Bureau of Trust Funds Administration (BTFA) to provide a capability to search a file folder level index of all inactive historical records that are retired to the American Indian Records Repository (AIRR), by centrally managing access to

inactive historical records that are dated back to the 1850's. The BISS helps BTFA (1) Create a file level listing of the contents of boxes containing inactive historical records, as a quick finding aid in the form of an index in place of the Standard Form (SF) 135, *Records Transmittal and Receipt*, created when inactive historical records are retired to the AIRR, (2) Provide authorized users with a tool to search a file level index of all inactive historical records, (3) Support research requests for copies of historical requests received from the original record owners, and conduct research on behalf of record owners in response to requests under the Freedom of Information Act (FOIA) and in support of litigation; and, (4) Track box inventories that accession retired inactive historical records into the National Archives and Records Administration (NARA).

The BISS serves as an indexing system locator tool and does not contain copies or contents of the original program files (documents) that are transferred from the originating office to the AIRR. The ownership of inactive historical records is retained by the originating office where the inactive historical records are created and are covered by applicable SORNs for the Privacy Act records. Requests for Privacy Act access to inactive historical records are processed in collaboration with the AIRR and the originating office as the data owner.

The BISS is associated with Versatile, a front end application that houses the BISS (e.g., Versatile/BISS). Versatile tracks processes associated with, (1) Records Move Requests (forms) which authorize boxes of inactive records to be moved from various field offices and programs to the AIRR, (2) SF 135, *Records Transmittal and Receipt* forms; (3) Box inventories of records that are accessioned, retired records into the NARA; and, (4) Research requests forms which are received from record owners requesting copies of documents stored at the AIRR.

The BISS and Versatile reside on the BTFANet. A Privacy Threshold Analysis (PTA) is being conducted for Versatile to assess if a full PIA is required. User identity information is originally collected by DOI Access via the consent and notice process. The data in the Department of the Interior DOI Active Directory (AD) is necessary for identity management and required under Federal mandates. The AD account information for user access is through Enterprise AD, which is assessed separately through the DOI's Enterprise Hosted Infrastructure (EHI). AD user account information includes names, passwords, and login time, data, and locality, and is used to authenticate user access and actions within EHI. The BISS does not contain the contents of program files that are transferred from the originating office to the AIRR and serves solely as a locator tool.

C. What is the legal authority?

44 U.S.C. 3101, Records Management by Agency Heads; 44 U.S.C. 3102, Establishment of Program Management; 44 U.S.C. 3102; 5 U.S.C. 301, Departmental Regulations; American Indian Trust Fund Management Reform Act of 1994, Pub. L. 103-412, 108 Stat. 4239; 25 U.S.C. 42, American Indian Trust Funds Management Reform; and Office of Management and Budget (OMB) M-12-18, *Managing Government Records*.

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:

E. Is this information system registered in CSAM?

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

The BISS is a minor application that resides on the BTFANet. The UII code is 010-000002654. A system privacy plan is being developed for BISS.

☐ No

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

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

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

☒ Yes:

INTERIOR/OS-3, Box Index Search System (BISS), July 29, 2005, 70 FR 43899; modification published February 13, 2008, 73 FR 8342. DOI SORNs may be viewed at: http://www.doi.gov/privacy/sorn. The existing SORN is currently being modified to include renaming and renumbering the SORN to INTERIOR/BTFA-02, BISS, to reflect the new BTFA organization and the second system of records maintained by BTFA.

The BISS does not actively collect personally identifiable information (PII) from individuals and does not maintain the contents of the file folders that are sent to AIRR. The ownership of inactive historical records is retained by the originating office within DOI where the records where created, and are covered by applicable bureau and office SORNs for the Privacy Act records.

☐ No

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

☐ Yes:

☒ No

There are no forms associated with the BISS. The BISS does not actively collect PII from individuals and does not maintain the contents (historical records) of the file folders that are sent to AIRR. The ownership of inactive historical records is retained by the originating bureau or office where the records where created.

Section 2. Summary of System Data

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

☒ Name
☒ Birth Date
☒ Tribal Affiliation
☒ Other Names Used
☒ Truncated SSN
☒ Education Information
☒ Social Security Number (SSN)
☒ Tribal or Other ID Number
☒ Mother's Maiden Name
☒ Mailing/Home Address
☒ Other:

The BISS system also contains case file number and date of death. PIV credentials and certificates or user name/password are required to access the network and BISS. User name/ display name are populated by the US/DOI Access system. Authorized users access the BISS using their AD credentials.

The BISS does not actively collect PII and does not maintain the contents of the file folders that are sent to AIRR. The ownership of inactive historical records is retained by the originating office where the records where created. There is PII on file folder labels that are created by the records owner. Inactive historical records stored at AIRR remain under the ownership of the originating office where the original records where created. Inactive historical records are accessioned into the AIRR.

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:

The BISS does not maintain Federal inactive historical records and does not actively collect PII from individuals. The sources of PII that are on the file folder labels are created by the original records owner or is obtained from other Federal agencies or organizations. DOI Access AD credentials are the source for employee PII collected during the hiring process. User name and password credentials are allowed when PIV card is unusable. AD contains user names and display names, and are populated by the US/DOI Access system.

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

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

The BISS does not maintain Federal inactive historical records and does not actively collect PII from individuals. The BISS shares information with Versatile, a front end application to the BISS regarding inactive records that are sent to the AIRR for storage. DOI Access (AD credentials) share PII with the BISS to provide access to the BISS. The BTFA/OST Service Now System shares information with BISS to support employee requests for access or Information Technology (IT) services.

☒ Other:

During the process for transferring/sending inactive records to the AIRR, PII may be initially provided throughout the records management process and transfer of records to the AIRR. There are no forms associated with the BISS. Original record owners may provide PII such as name, SSN, and date of birth in research requests which will help AIRR locate the historical records. PII shared during face-to-face contact from other AIRR staff who work in close proximity to each other on a regular basis. PII is associated with records contained in file folders in boxes of inactive historical records that are shipped to the AIRR by the original record owner via commercial courier, i.e., Federal-Express (Fed-Ex) or United States Postal Service (USPS).

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

The BISS does not actively collect PII from individuals. The intended uses of PII are as identifiers to enter and index file folder labels into the BISS; to search and locate inactive historical records by the file folder label; use when processing research requests; to support responses to the Privacy Act, FOIA, and litigation by searching for responsive documents that may be associated with file folder labels containing PII.

The BISS resides on the BTFANet GSS. The GSS does not collect or process PII, serves as a conduit, transfer point for interface files to share information, and supports BTFA's mission. BTFANet provides hosting services to BTFA for mission support operations. PII associated with employee's and contractor's may be used for authorized access to the DOI network or for business use from other sources (applications) to create work products (reports, analytical spread sheets, etc.) via office automation tool such as MS Office. PII associated with AD contains user name and display name, populated by the US/DOI Access system.

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

☒ Within the Bureau/Office:

The BISS is shared with authorized users to search a file level index of all inactive historical records that are retired to the AIRR.

☒ Other Bureaus/Offices:

PII may be shared with other DOI Bureaus/Offices including the Bureau of Indian Affairs (BIA), Bureau of Indian Education (BIE), Office of Justice Services (OJS), Office of the Secretary (OS), Office of the Solicitor (SOL), Office of Inspector General (OIG), Office of Hearings and Appeals (OHA), and Office of Natural Resource and Revenue (ONRR) in the performance of official duties.

☒ Other Federal Agencies:

PII may be shared with the Department of Justice (DOJ), Government Accountability Office (GAO), and other Federal Agencies as necessary to support BTFA and DOI's mission, business functions, and to conduct annual internal or financial audits.

☒ Tribal, state or local agencies:

PII may be shared with Tribes who are authorized to search the BISS for the purpose of retrieving responsive historical records to satisfy litigation and non-litigation requests, including Privacy Act, FOIA requests, and litigation.

☒ Contractor:

PII may be shared with contractors (and employees of the contractor) who are authorized to search the system for the purpose of retrieving responsive historical records to satisfy litigation and Privacy Act, and FOIA requests non-litigation requests, or to perform services for BTFA that requires access.

☐ 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:
☒ No:

The BISS does not collect PII from individuals, and individuals do not provide consent for specific uses of their PII on file folder labels. File folder labels may contain PII that was created by the originating record owners before they were sent to the AIRR for storage as inactive records.

The PII associated with the BTFANet is originally collected by DOI Access via the consent and notice process. Individuals are required to agree to provide consent to use in order to gain access to the BISS and overall DOI network. Authorized users are provided an AD account through the employee onboarding process and access request forms, and would not have an AD account without 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:

Privacy notice is provided through the publication of this PIA and the INTERIOR/OS-3, Box Index Search System (BISS), SORN which is under revision. The current BISS SORN may be viewed on the DOI Office of the Secretary SORN website at https://www.doi.gov/privacy/sorn.

☒ Other

At logon to the network users and system administrators receive the DOI security banner that notifies all authorized users (holders of both regular and administer accounts) of the system and DOI network that they are accessing a DOI system, are subject to monitoring, and there is no expectation of privacy during use of the system.

☐ None

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

Identifiers associated with the BISS, file folder labels may include:

- Name, other names used, or maiden;
- Type of inactive historical records in the folder;
- Location of where inactive historical records originated;
- Date ranges of the information;
- Records management information;
- Miscellaneous information associated with the inactive historical records storage box;
- Mailing and/or home address;
- Social Security number (SSN);
- Case file number;
- Tribe, Tribal affiliation, Tribal enrollment or census number;
- Date of birth and/or date of death;
- Tax identification number;
- IIM account number; and,
- School name or educational institution.

The BISS does not maintain the contents of the boxes within the file folder(s). Inactive historical records that are retired to the AIRR may be covered by other applicable SORNs established by the bureau where the records originated.

I. Will reports be produced on individuals?

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

The BISS may produce reports associated with the file folder labels that may include PII. It only contains information that is on each file folder label within a box of inactive records that are indexed and maintained at the AIRR FRC. Audit reports are associated with system audit logs that tracks user activity in accordance with DOI logging requirements. Logged information is used for investigative actions associated with cyber security incidents.

☐ No

Section 3. Attributes of System Data

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

The BISS does not actively collect new data from other sources. During the process for transferring/moving inactive historical records to AIRR, inventories of each file folder label within the boxes of inactive historical records are verified for accuracy before arriving at AIRR by following established processes which include quality review as the files and documents are indexed and as needed by authorized users. The quality review process also includes verifying that all captured data has been collected accurately, as well as, verifying that the quantity and order of files in a box matches what was entered into the front end of the BISS by Versatile, the front end application to the BISS.

PII is originally collected by DOI Access via the consent and notice process. Authorized users are required to agree to provide consent to use in order to gain access to the BISS and overall DOI network. Employee PII is verified during the on-boarding process and through the access request form(s). Employee on-boarding is a process handled by the servicing personnel office for BTFA as part of the hiring process.

B. How will data be checked for completeness?

File folder labels contained within the BISS include a manal pre- and- post quality review process to ensure that all file folder labels are indexed accurately, along with the quantity and order of files in a box. File folder labels, information (data) is also checked for completeness by the records custodians at the time of submission, and as owners of the inactive historical records during the process to transfer inactive historical records to the AIRR.

Employee PII is originally collected by DOI Access in order to gain access to the BISS and overall DOI network. Data is checked for completeness during the employee on-boarding process and through the access request form(s). Generally, employee onboarding is a process that is handled by the personnel office for BTFA at the time of hire.

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

None of the data on file folder labels is current. The BISS creates an index of inactive historical records that are retired to the AIRR. File folder labels are indexed following a process which ensures all files and document information is captured accurately. As file folder label information is entered it goes through a quality review process for verification.

Employee PII and data that is originally collected by DOI Access is checked for completeness during the employee on-boarding process and through the access request form(s). Generally, employee onboarding is a process that is handled by the personnel office for BTFA at the time of hire. Employee user data is also kept current by daily updates from the AD and asset inventories are updated annually as required by annual ongoing authorization.

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

Retention periods vary according to agency needs and specific subject matter, and are retained in accordance with the applicable Indian Affairs Records Schedule (IARS) and the Departmental Records Schedule (DRS) approved by the NARA. Record retention periods may also be suspended by litigation holds, court orders, preservation notices, and similar limitations on records disposition issued by the Office of the Solicitor, the DOI Records Officer, or other authorized official.

Within the BISS, information associated with the Box Number, Box Title, Box Source, Tribes identified, File Title and Document Types are covered by IARS 6013-BISS. The disposition for these records are permanent. Permanent records that are no longer needed for agency use are transferred to NARA for permanent retention in accordance with NARA guidelines. Subsequent legal transfer of the records will be as jointly agreed to between DOI and NARA, in accordance with regulations currently cited in 36 CFR 1228.270.

Copies of records related to vital record backups are covered by DRS 1.4.0013, Short-term IT Records, and system security are covered by DRS 1.4.0014, System Planning, Design, and Documentation. Disposition for records that are covered by DRS 1.4.0013 and DRS 1.4.0014 have a temporary disposition. These records are destroyed/deleted 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?

Permanent records are transferred to NARA in accordance with the disposition instructions. Subsequent legal transfer of the records will be as jointly agreed to between DOI and NARA, in accordance with regulations currently cited in 36 CFR 1228.270. Approved disposition methods are in accordance with NARA instructions and guidance. Approved destruction methods for temporary records that have met their retention period include erasing or degaussing electronic records in accordance with NARA guidelines and Departmental policy.

Electronic records are deleted; temporary records are shredded or pulped; backup tapes are reinitialized and reused. Employee exit clearance process documents the steps and procedures used to remove or archive information when employees or contractors leaves BTFA. 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 moderate privacy risk to the privacy of individuals due to the file folder labels, volume of PII that is contained in the BISS. This risk is mitigated by a combination of technical, physical, and administrative controls that are implemented to protect the confidentiality, integrity, and availability of the information; and, data is safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy requirements and policies. System Administrators and authorized users, including contractors ensure the handling of PII is consistent with government-wide and agency policies and follow the OMB policies and National Institute of Standards and Technology (NIST) guidelines for information management. Security is also provided through and combination of technology, management and operational controls.

There is a risk that data may be used for unauthorized purposes. DOI authorized personnel must sign the DOI Rules of Behavior (RoB) and are subject to monitoring of the BISS and DOI network. Failure to protect misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, or administrative penalties. DOI employees must take Cybersecurity, Privacy, Records Management, Section 508 Compliance, Controlled Unclassified Information Reference Guides training prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take Role-Based Training (RBPT) initially and annually, to ensure an understanding of the responsibility to protect privacy. The System Administrator reviews the use of the system to ensure that the system is not improperly used and to prevent unauthorized use or access, and assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

The BISS resides on BTFANet, formerly OSTNet, which has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and NIST. The BTFANet is rated as a FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII and other sensitive information contained in the system. The BTFANet has developed a System Security and Privacy Plan based on NIST guidance and is part of a Continuous Monitoring Program (CMP) that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. As part of the CMP continual auditing occurs on the GSS to identify and respond to potential impacts to PII information stored within the environment, which will help the agency effectively maintain a good privacy and security posture for the system. The audit trail records security relevant events and includes the identity of each entity accessing the system, time and date of access (including activities performed using a system administrator's identification) and activities that could modify, bypass, or negate the system's security controls. Data is protected through user identification, passwords, database permissions, and software controls. System security measures establish different access controls for different types of users associated with pre-defined groups and/or bureaus. 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.

There is a risk that individuals may not receive adequate notice of DOI privacy practices or the extent of the use of their PII data in BISS. The BISS does not collect information directly from individuals. Privacy Notice is provided through the publication of this privacy impact assessment and the INTERIOR/OS-3, Box Index Search System (BISS), SORN. The SORN is currently under revision. Individuals may contact DOI privacy officials with any questions or privacy concerns.

There is a risk that information in the BISS, BTFA and DOI information system or applications will be maintained longer than necessary to achieve the BTFA and DOI mission, or that records may not be properly destroyed. The records in BISS have a permanent retention due to their historical value. This risk is mitigated by securely managing records and accessioning the records in accordance with a NARA-approved records schedule, and providing extensive training to users on IT security, Privacy, Records Management and controlled unclassified information. This training specifically includes handling and disposal of records with sensitive information and also the proper procedures for handling faxed information.

There is a risk associated with sharing data with the AD. This risk is mitigated through data validation checks in place for AD to identify any discrepancies such as incomplete or duplicated data. The use of BTFA IT systems is conducted in accordance with the appropriate BTFA use policy. All access is controlled by authentication methods to validate the authorized user.

Other potential privacy risks identified include inadvertent disclosure, unauthorized access, surveillance and theft of data. The risk is mitigated through security and privacy controls to protect the system and data. Any unauthorized disclosure may reveal details of an individual's IP address, contact information and service request history. All data is stored and maintained in secure systems and is protected from unauthorized access by firewalls, intrusion detection systems, antivirus and the AD domain environment. User activity is monitored and logged to ensure only appropriate use of the system and data. To mitigate the insider threat, collected data is protected by access controls including two-factor authentication, least privilege principles and restricted access limited to authorized users. 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 must comply with the principles of separation of duties.

There is a risk that file folder labels containing PII may not be accurate. Information in BISS is obtained from historical records. Data associated with individual's information is verified for relevance or accuracy by authorized users. Data received from original record owners must be accurate before they are sent to the AIRR for storage. The BISS resides on the BTFANet and does not create new data. AD and DOI Access have data validation checks in place to identify any discrepancies such as incomplete or duplicated data.

All BTFA employees must take privacy, security, and records management training prior to being granted access to BTFA information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure and understanding of the responsibility to protect privacy. BTFA personnel also sign the 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:

The BISS allows for the location of copies of responsive inactive records for use with non-litigation, litigation and FOIA research, as well as, assisting BTFA in achieving the safeguarding of Indian records as set forth in the BTFA Strategic Plan and compliance with OMB M-12-18, *Managing Government Records*. Therefore, the data are relevant and necessary to the purpose for which BISS was designed.

☐ 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: *Explanation*

☒ No

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

N/A. The BISS does not derive new data or create previously unavailable data about an individual through data aggregation. File folder label information that is entered into the BISS is verified for relevance and accuracy by authorized users.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☒ 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?

Auditors may have access to data associated with annual reviews or audits. User access is controlled by system profile and based on roles and responsibilities. Access to the data is restricted to authorized personnel based on official need-to-know basis and as required to perform official duties. Data that is indexed is protected through user identification, passwords, database permissions, and software controls. There are security measures established at different access levels for different types of users associated with pre-defined groups and/or bureaus. Only the BISS administrator(s) have access to all data within the system for the purpose of managing and administering user accounts and content, and must follow established internal security protocols, complete all security, privacy, and record management training, and sign the BTFA Rules of Behavior.

The BISS resides on the BTFANet. User access is limited to the applicable systems within the applicable or associated offices or programs. User access is also controlled by system profile and based on roles, responsibilities and access requests from data owners. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. Access to data is restricted to authorized users and personnel who have a need to know to perform their duties. Access is further governed by DOI and BTFA IT security policy, including limited access rules, various firewalls, and other protections put into place to assure the integrity and protection of personal information.

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.

Appropriate Privacy Act clauses are included in the contract.

☐ No

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

☐ Yes.

☒ No

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

☒ Yes.

Authorized user actions and use of the system are monitored to meet BTFA security policies. Data captured includes the user's last date of login, date of user content creation, and date user content was modified. Routine file maintenance 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.

The BISS resides on the BTFANet. Data input and changes can be tracked. All user activity is audited as part of the security monitoring and management of user accounts and can be reviewed by Security personnel; the audited information includes items such as: failed login/access attempts, changes in user permissions, etc., that are associated with user authentication.

☐ No

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

The BISS does not have the capability to monitor individuals. As part of the security monitoring and management of the system, all user actions taken on BTFA IT systems are audited by system administrators. This information includes items such as username, login date/time/location, failed login/access attempts, changes in user permissions, and other items associated with user authentication. Suspicious events, such as excessive unsuccessful attempts to log in, unusual network traffic, or any potential compromise of PII, are reported immediately upon detection, for investigation and escalation if necessary.

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

The BISS is not intended to monitor individuals; however, the system has the functionality to audit the usage activity. 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. The system administrator(s) review the use of the BISS and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. The system administrator(s) assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place. Federal employees and contractors must complete annual security and privacy awareness training, and role-based training, and sign the BTFA Rules of Behavior before access is granted. Authorized contract employees are monitored by their Contracting Officer (CO) and Associate Chief Information Officer (ACISO).

All access activity (e.g., unsuccessful login attempts, date/time of access, etc.) and changed to system activity. Audit logs capture who was on the system, the date, and time stamps. The BISS resides on the BTFANet, and 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, 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.

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. Badged Access Control.

(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 AIRR Director is the Information System Owner (ISO) and is the official responsible for oversight and management of the BISS security controls and the protection of information processed and stored by the system. The ISO and Information System Security Officer (ISSO) share responsibility for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the BISS, in consultation with BTFA and DOI privacy officials.

The ISO and System Manager are responsible for protecting individual privacy for the information collected (if applicable), maintained, and used in the system, and for working with the Privacy Act system manager to meet the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with the BTFA Associate Privacy Officer (APO).

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 Director for the AIRR is the ISO and is responsible for the daily operational oversight and management of the BTFANet 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 ISO and ACISO, and authorized users 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 1-hour of discovery in accordance with Federal policy and established DOI procedures, and for working with the BTFA APO and Departmental Privacy Office to ensure appropriate remedial activities are taken to mitigate any impact to individuals.