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: Digital Center for Excellence
Bureau/Office: Bureau of Trust Funds Administration
Date: July 15, 2022
Point of Contact
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: BTFA_Privacy@BTFA.gov
Phone: (505) 818-1645
Address: 4400 Masthead Street Northeast, 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: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Bureau of Trust Funds Administration (BTFA) is developing the Digital Center for Excellence (DCE). The system supports the BTFA Electronic Records Management Program (ERMP), consists of inactive and retired DOI records stored at the American Indian Records, Repository (AIRR) located in Lenexa, Kansas, Federal Records Center (FRC), supports the BTFA archiving and research mission, maintains an electronic storage of retired records for

efficient retrieval, serves as a digital repository to house images, allows for the search and retrieval of digital records, document text to be searchable, and copies meta-data into the documents. The system retrieves responsive images of approved and appropriate data to satisfy litigation, non-litigation, and Freedom of Information Act (FOIA) requests. This privacy impact assessment (PIA) covers the DCE system of records, BJL|AI, and the Gateway Portal.

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; 5 U.S.C. 301, General Departmental Regulations, 44 U.S.C. Chapter 36, Section 208, Management and Promotion of Electronic Government Services, 36 CFR 1220: Federal Records Act, Office of Management and Budget (OMB) M-12-18, *Managing Government Records,* OMB Circular A-130, *Managing Information as a Strategic Resource,* Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service,* Clinger–Cohen Act of 1996, 40 U.S.C. 1401, and Presidential Memorandum, *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: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: UII: 010-000002837; DCE System 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.*
BJL|AI	The BJL|Artificial Intelligence (AI) is a system that uses AI to improve and provide	Yes	Name, Gender, Birth Date, Marital Status, other Names Used, Social Security number,

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	Optical Character Recognition (OCR) of documents, copy meta-data into the documents, and export an archival quality copy of the image to DOI's Azure environment.		Legal Status, Place of Birth, Security Clearance, Financial Information, Medical Information, Disability Information, Law Enforcement, Education Information, Emergency Contact, Driver's License, Race/Ethnicity, Personal Cell Telephone Number, Tribal or other ID Number, Personal Email Address, Mother's Maiden Name, Home Telephone Number, Child or Dependent Information, Employment Information, Military Status/Service and Mailing/Home Address.
Gateway (Portal)	The Portal is a digital records interface that accesses archival quality digital images from blob storage inside the DOI's Azure environment. This system allows for the searching and retrieval of digital records, data extracted from the records OCR, and additional metadata inserted at the time of scanning.	Yes	Same as above.

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

☒ Yes: *List Privacy Act SORN Identifier(s)*

The system does not collect personally identifiable information PII) from individuals. The system contains retired DOI records as the official retired record. The retired DOI records are under the control and ownership of the originating records custodian, system of records owner, or Privacy Act system manager, and may be covered under numerous government-wide, DOI bureau/office, other Federal Agency system of records notices (SORNs), including the INTERIOR/OS-02, Individual Indian Money (IIM) Trust Funds, and 84 FR 44321 (August 23, 2019), and INTERIOR/OS-03, Box Index Search System (BISS), 70 FR 43899 (July 29, 2005); modification published February 13, 2008, 73 FR 8342. The INTERIOR/OS-03 BISS SORN is currently undergoing an amendment. The SORNs may be viewed at: https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes: *Describe*

☒ No

The system does not collect PII from individuals. Due to the nature of DCE as BTFA's repository of retired records, there may be numerous OMB control numbers for any information collection from the original records. The digitized records (images) remain under the control and ownership of the originating records custodian, system of records owner, or Privacy Act system manager.

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information

☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ 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
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: The PII is not collected from individuals. Due to the nature of DCE as BTFA's repository of retired records, records may include various types of PII or other information about individuals that is contained in DOI records. The originating DOI records (the digitized images) are under the control and ownership of the originating records custodian, system of records owner, or Privacy Act system manager.

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 PII is not collected from individuals. The system is associated with inactive historical records that have been retired to the AIRR. There may be numerous sources of PII for the original records. The retired DOI records are under the control and ownership of the originating records custodian and may be covered under numerous government-wide, DOI bureau/office, and other Federal Agency SORNs including the BTFA Interior/OS-02, IIM Trust Funds and INTERIOR/OS-03, BISS. The SORNs may be viewed at: https://www.doi.gov/privacy/sorn.

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*
☒ Other: The system does not collect PII from individuals. The system is associated with retired DOI records that have been transferred to the AIRR, FRC, and remain under the control and ownership of the original record owner. The Gateway Portal is an electronic record repository housing digital images and allows document text to be searchable.

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

The system does not collect PII from individuals. The system functions as a digital research and distribution center, serves as a nationwide records storage and archival processing center. Authorized users retrieve responsive images to satisfy litigation, non-litigation, and FOIA requests.

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

☒ Within the Bureau/Office: Authorized BTFA users research and retrieve responsive images to satisfy litigation, non-litigation, and FOIA requests. The images may be used for document production purposes or document collections may be reviewed to determine what needs to be redacted and what is appropriate for disclosure depending on the type of request. Data in the system may be used for security and privacy incidents reported to the DOI-CIRC and the Department of Homeland Security (DHS) US-CERT and may be shared internally or with other law enforcement agencies for investigative purposes.

☒ Other Bureaus/Offices: The digitized record image(s) may be shared with other DOI Bureaus/Offices to fulfill DOI's mission. The images may be used for document production purposes or document collections may be reviewed to determine what needs to be redacted and what is appropriate for disclosure depending on the type of request. Data may be shared with other DOI Bureaus/Offices as authorized and required to meet legal and reporting requirements. Data in the system may be used for security and privacy incidents reported to the DOI-CIRC and the DHS US-CERT and may be shared internally or with other law enforcement agencies for investigative purposes.

☒ Other Federal Agencies: Inactive records containing PII may be shared with other Federal agencies in the performance of official duties. The images may be used for document production purposes or document collections may be reviewed to determine what needs to be redacted and what is appropriate for disclosure depending on the type of request. Data may be shared with

other Federal agencies as authorized and required to meet legal and reporting requirements. Data in the system may be used for security and privacy incidents reported to the DOI-CIRC and the DHS US-CERT and may be shared internally or with other law enforcement agencies for investigative purposes.

☒ Tribal, State or Local Agencies: Inactive records containing PII may be shared with Tribes who are authorized to access or receive data from the system to satisfy litigation and non-litigation or in response to FOIA and Privacy Act requests. Data may be used for security and privacy incidents that are reported to the DOI-CIRC and the DHS US-CERT, and may be shared internally or with other law enforcement agencies for investigative purposes.

☒ Contractor: Inactive records containing PII may be shared with contractors (and employees of the contractor) who are authorized to access the system to provide operational support for the system, or to satisfy litigation and non-litigation including, responses to FOIA and Privacy Act requests. Data may be used for security and privacy incidents that are reported to the DOI-CIRC and the DHSUS-CERT, and may be shared internally or with other law enforcement agencies for investigative purposes.

☒ Other Third Party Sources: Inactive records containing PII may be shared with external auditors or the Office of the Inspector General (OIG) in the performance of annual or financial audits. Data may be used for security and privacy incidents that are reported to the DOI-CIRC and the DHS US-CERT, and may be shared internally or with other law enforcement agencies for investigative purposes.

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

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: The system does not collect PII from individuals. The data consists of digitized images of retired records that are accessioned to the AIRR. Individuals do not have an opportunity to decline to provide their personal information. Consent was provided when the original record was created by the record owner.

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

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this PIA and the related SORNs that cover the original records.

☒ Other: Authorized users receive a warning banner when they logon to DOI/BTFA Information Systems.

☐ None

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

Metadata can be searched or retrieved by any word in the document. Identifiers may include the following: Name, religious preference, SSN, citizenship, security clearance, personal cell, telephone number, gender, spouse information, Tribal or other ID number, birth date, financial information, personal email address, group affiliation, medical information, mother's maiden name, marital status, disability information, biometrics, credit card number, child or dependent information, other names used, law enforcement, employment information, truncated SSN, education information, military status/service, legal, status, emergency contact, mailing/ home address, place of birth, date of death, driver's license, race/ethnicity. Due to the nature of DCE as BTFA's repository of retired records, records may include various types of other PII on about individuals that are contained in original DOI records.

I. Will reports be produced on individuals?

☒Yes: Reports may be produced for audit, administrative, or for official reporting purposes. Authorized officials have access to reports in the performance of their official duties. Audit logs track user activity in accordance with DOI and BTFA logging requirements. The logged information may be used for investigative actions associated with Cyber Security and Privacy incidents that are reported to DOI-CIRC, internal organizations, or other external organizations, as necessary.

☐No

Section 3. Attributes of System Data

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

The system is associated with retired DOI records that are transferred to and stored at the AIRR by the record owner (record custodian) and does not collect new data. The retired records were verified for accuracy by the submitting DOI bureau/office. There is a quality review process to ensure that digitized records have captured the entire retired record content. The Gateway Portal associated with the system serves as a digital repository that houses images of records that are accessioned to AIRR and allows the document text to be searchable.

B. How will data be checked for completeness?

None of the data is current. The system does not collect new data from individuals. The data exists from the transfer of retired records that are stored at the AIRR and are checked for completeness by the submitting DOI bureau/office.

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 is current and are static in time. The retired DOI records were accessioned and transferred into the AIRR for storage and go through a quality review process to ensure accuracy as images are scanned and entered into the digital repository.

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

The system does not create new records, does not maintain active DOI records, and no new information is collected from individuals. The digital repository will maintain scanned images of retired records that were sent to the AIRR for permanent retention and storage. The data will be retained in accordance with the applicable Departmental and bureau/office records schedule approved by the National Archives and Records Administration (NARA).

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

Digitized records maintained by the system will follow the applicable disposition instructions in accordance with the NARA approved Records Disposition schedule. The system maintains electronic storage of records, functions as a digital research, and distribution center for retired records.

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 may be a privacy risk to individuals due to the nature of the type of digitized inactive retired DOI records maintained by the system. These risks are mitigated through a variety of security and privacy controls that protect the data. The principle of least privilege is observed during all phases of the information lifecycle. The potential privacy risks identified include inadvertent disclosure, unauthorized access, and surveillance or theft of data. The system is secured and protected from unauthorized access by firewalls, intrusion detection, and antivirus. User activity is monitored and logged to ensure appropriate use of the data.

To mitigate insider threat, the data is protected by access controls, including two-factor authentication, and restricted access limited to authorized users. Employees are required to complete annual Information Management and Technology (IMT) Awareness Training, which includes privacy and security training, and affirm the BTFA Rules of Behavior. Those with access to PII are required to also complete mandatory role-based privacy training

annually. BTFA computers are secured and monthly scans are conducted in accordance with the BTFA Continuous Monitoring Plan.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The system is provided and hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with Federal Information Security Modernization Act of 2014 (FISMA). The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data at the moderate level. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and National Institute of Standards and Technology (NIST guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that the system may collect, store or share more information than necessary, or the data will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. To mitigate the risk, data maintained in the system is limited to the minimal amount of data needed to meet Federal records requirements and the applicable retention schedules.

There may be a risk that contractors may not handle information according to DOI policy. To mitigate any risk, a system security and privacy plan was completed to address security controls and safeguards for the system. Controls are outlined in the System Security and Privacy Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, and includes the requirements for awareness and role-based training, encryption, and maintaining data in secure facilities, among others. The system implements audit logging mechanisms for the information systems and its applications. Audit logging is utilized to assess system security posture in the identification of potential incidents or compromised systems by monitoring for vulnerabilities that lead to breaches. Risk assessments have been conducted and includes the likelihood and magnitude of harm resulting from unauthorized events such as unauthorized access, use, disclosure, disruption, modification and destruction of data. The risk assessment results are documented in the security assessment report (SAR).

There is a risk that individuals may not receive adequate notice. Individuals are provided notice through the publication of this PIA and the applicable SORNs that cover the original records. Additionally, authorized users receive a warning banner when logging on to DOI/BTFA Information Systems.

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 use of the data maintained by the system allows BTFA to manage and preserve retired records to meet accountability and archival obligations under the Federal Records Act, and for compliance with OMB-12-18, *Managing Government Records*. The system addresses concerns such as preventing the loss of records that should be kept for legal and accountability

purposes, achieving confidence in the authenticity and reliability of records (images), eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records (images) inaccessible or incomprehensible.

☐ No

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

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

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable. The system does not collect or maintain new data and will not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

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

BTFA uses Role-Based Access Control (RBAC) through Active Directory (AD) and the use of Group Policy Objects (GPO) so that users do not have discretionary access to enterprise objects. Access permissions are administratively associated with roles, and users are administratively made members of appropriate roles for access to electronic records systems.

Auditors may have access to data associated with annual review or audits. User access is controlled by system profile and based on roles and responsibility. Access to the data is restricted to authorized personnel based on official need-to-know basis and as required to perform official duties. Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view or access. Access is further governed by DOI IT security and privacy policy, including the use of assigned passwords, limited access rules, various firewalls, and other protections put into place to ensure the integrity and protection of information. All DOI employees and contractors undergo initial and annual security, privacy, and records management training, and sign the DOI/BTFA Rules of Behavior.

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

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

Contractors are involved with the design and configuration of the system and in the maintenance and operation of the system. The Federal Acquisition Regulation (FAR) Contract Clauses for Privacy Act Notification, Privacy Act, and Privacy or Security Safeguards are included in the contract(s) associated with system.

☐ No

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

☐ Yes. *Explanation*

☒ No

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

☒ Yes. *Explanation*

Authorized user actions and use of the system are monitored to meet BTFA security policies. The system has the ability to audit usage of the system, including reviewable data concerning logins, include login time to protect against unauthorized access or actions within the system. Audit logs, access level restrictions, and least privilege are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized access or actions within the system. Routine file maintenance audit records are maintained that identify when account asset name/address information is created maintained/changed and deleted. Firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators review activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

☐ No

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

As part of the security monitoring and management of the system, all user actions taken on system 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.

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

Access is limited to authorized users who have a need to access the data in the performance of their official duties. Access to the system must be approved by the system owner or system administrator before access is granted. Access activity, e.g., unsuccessful login attempts, data/ time of access, etc., and system activity. All changes are logged by the system and audit logs are used to prevent unauthorized monitoring.

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*

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 Director for the AIRR is the Information System Owner (ISO). The ISO, Information System Security Officer (ISSO), and the BTFA Associate Privacy Officer (APO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in accordance with Federal laws and policies for the data managed, used, and stored in system. The system manager, in coordination with the APO are responsible for protecting the privacy rights of the individuals. The system vendor and cloud service provider are also responsible for the protection of PII, incident reporting, and other security and privacy controls to ensure adequate safeguards are implemented in accordance with the appropriate Federal laws, regulations, and Departmental policies.

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 and ISSO are responsible for oversight and management of the system security and privacy controls and are responsible for ensuring to the greatest extent possible that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. All authorized users are responsible for reporting 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, and for working with the BTFA APO and Departmental Privacy Office to ensure appropriate activities are taken to mitigate any impact to individual.