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: FTI Indian Trust Information System (FTIS) Decommissioning
Bureau/Office: Bureau of Trust Funds Administration
Date: September 30, 2022
Point of Contact
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: btfa_privacy@btfa.gov
Phone: (505) 816-1645
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), formerly known as, the Office of the Special Trustee for American Indians (OST), in the Office of Historical Trust Accounting (OHTA), planned and directed the historical accounting of Individual Indian Money (IIM) and tribal

accounts, supported DOI and Department of Justice (DOJ) in litigation and settlement claims, and provided litigation support in analyzing and reconciling the historical collection, distribution, and disbursement of income from IIM accounts, Indian trust land, and other revenue sources. OHA used the FTI Indian Trust Information System (FITIS) to perform tests of the legacy accounting systems and to reconcile Indian Trust transactions.

FITIS users performed these analyses by querying historical account and transactional data. FITIS provided a secure, central data repository to hold all historical data and as well as the results of analyses. The data reviewed consisted of copies of lease records, ownership information, transaction and payment records to individual Indians and tribes, and investment data. These records contained information considered sensitive and confidential and, therefore, are protected under Federal Privacy Act guidelines. Personally Identifiable Information (PII) was also used to resolve class membership questions related to litigation claim settlement

FITIS was taken offline, decommissioned, and is no longer in use to collect or maintain PII. A decommissioning plan was completed to outline and document the procedures and to ensure the system was decommissioned in a secure and auditable manner. FITIS files and SQL databases have been transferred to the Net IQ, a local security network shared drive. All FITIS permanent data was archived onto a hard drive that is stored at the American Indian Records Repository (AIRR), Federal Records Center (FRC). System documentation is stored on BTFA shared drives in accordance with DOI records management policies. Data sanitization was completed and documented on the DI-1941, Documentation of Temporary Records Destruction form.

C. What is the legal authority?

American Indian Trust Fund Management Reform Act of 1994, Pub. L. 103-412, 108 Stat. 4239.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☒ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

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

UII: 01-000000703; FITIS 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.*
N/A	N/A	N/A	

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)*

INTERIOR/OS-02, Interior, Individual Indian Money (IIM) Trust Funds SORN, 84 FR 4321 (August 23, 2019), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/os-notices.

☐ No

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

☐ Yes: *Describe*
☒ No

The system was decommissioned and no longer collects or maintains information from individuals.

Section 2. Summary of System Data

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

☒ Other: The system was decommissioned and no longer collects or maintains PII on individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at 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 system was decommissioned and no longer collects or maintains PII on individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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 was decommissioned and no longer collects or maintains PII on individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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

The system was decommissioned and no longer collects or maintains information on individuals. PII data previously collected supported OHTA's mission to plan and direct the historical accounting of IIM and Tribal accounts, as well as DOI and DOJ for litigation purposes. However, the system was taken offline and does not collect PII.

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

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

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

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

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

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

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

The system was decommissioned and no longer collects or maintains PII on individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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 was decommissioned and no longer collects or maintains PII on individuals. The data in FITIS was obtained from existing DOI records and is not collected directly from individuals.

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.*

☐ Other: *Describe each applicable format.*

☒ None

Not applicable. The system was decommissioned and no longer collects or maintains PII on individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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

The system was decommissioned and no longer collects or maintains information from individuals. Therefore, data is not retrieved from the system. All FITIS permanent data is stored at AIRR.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

Not applicable. The system was decommissioned and no longer collects or maintains information from individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

B. How will data be checked for completeness?

Not applicable. The system was decommissioned and no longer collects or maintains information from individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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

Not applicable. The system was decommissioned and no longer collects or maintains information from individuals. FITIS files and SQL databases were transferred to Net IQ. All FITIS permanent data is stored at AIRR.

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 was decommissioned and taken offline. The database maintained historical information that provided government information on tribes/individuals. These historical records were maintained under the applicable Departmental Records Schedule (DRS), General Records Schedule (GRS), or the Indian Affairs Records Schedule (IARS), which were approved by the National Archives and Records Administration (NARA) for the appropriate record type(s).

The system was not scheduled at the time of system development. Therefore, the data associated with this system are considered permanent records and transferred to AIRR since it has been decommissioned.

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

The system has been decommissioned. PII is no longer collected by the system. Approved disposition methods include degaussing or erasing for electronic records are in accordance with NARA Guidelines and Departmental policy. Storage devices were excessed, and drives shredded in accordance with DOI policy or received sanitization, verification, and certification services. Data sanitization was documented on the DI-1941, Documentation of Temporary Records Destruction form.

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.

The system was decommissioned. PII was not collected by the system. There was a limited privacy risk for the decommissioning of the system related to potential unauthorized access or mishandling of the data. A decommissioning plan was completed to outline and document the procedures and to ensure the system was decommissioned in a secure and auditable manner. FITIS files and SQL databases have been transferred to the Net IQ. All FITIS permanent data was archived onto a hard drive that is stored at AIRR. System documentation is stored on BTFA shared drives in accordance with DOI records management policies. Data sanitization was completed and documented on the DI-1941, Documentation of Temporary Records Destruction form. No data was migrated to or maintained in other DOI or BTFA 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: *Explanation*
☒ 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?

The system was decommissioned and PII is no longer collected or maintained by the system.

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: The system was decommissioned, and PII is no longer collected or maintained by the system.

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

The system was decommissioned and PII is no longer collected or maintained by the system.

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?*

☒ 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*
☒ No

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

Not applicable. The system was decommissioned, and PII is no longer collected or maintained by the system.

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

Not applicable. The system was decommissioned, and PII is no longer collected or maintained by the system.

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. The system was decommissioned. No data was migrated or maintained in other BTFA/DOI systems.

(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. The decommissioning plan provides details on the disposal of the information technology resources. No data was migrated or maintained in other BTFA/DOI systems.

(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. The decommissioning plan provides details on the disposal of the information technology resources. No data was migrated or maintained in other BTFA/DOI 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 Director of the BTFA Office of Business Management is the Information System Owner and the Information System Security Officer manage the security controls in the system. These officials are responsible for ensuring appropriate security and privacy controls are implemented and managed in accordance with Federal and DOI policy. The BTFA Associate Privacy Officer (APO) is responsible for addressing privacy related complaints.

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 System Owner and Information System Security Officer are responsible for managing the security and privacy controls in the system and ensuring proper use of the system and data. These officials and the BTFA APO are responsible for reporting any loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information to DOI-CIRC, DOI's incident reporting portal l, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals.