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: Accounting Reconciliation Tool (ART)
Bureau/Office: Office of the Special Trustee for American Indians (OST), Office of Historical Trust Accounting (OHTA)
Date: September 1, 2017
Point of Contact: ART Program, System Manager
Name: Colleen Stegner
Title: ART Program Manager
Email: colleen_stegner@ost.doi.gov
Phone: (202) 208-5671
Address: 1849 C Street, NW, Room 3218, Washington, District of Columbia, 20240

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 Accounting Reconciliation Tool (ART) directly supports the OST Office of Historical Trust Accounting's (OHTA) mission to plan and direct the historical accounting of Individual Indian Money (IIM) accounts, as directed by Cobell v. Norton. The ART assists Government selected accounting firms in reconciling IIM accounts. ART is a GOTS desktop application with image accessibility through web services.

The ART allows accountants at the various firms to use a common system to query transactions from legacy data sources; link these transactions to relevant source document images; then reconcile these transactions and note any discrepancies, where appropriate. In addition, the ART assists the Government in performing quality control functions and to monitor the reconciliation activities. Statisticians analyze the reconciled transactions to determine an assurance level and calculate the potential level of monetary exposure. The ART is also used to search for images of documents and perform analysis related to litigation in support of the DOI's Office of the Solicitor (SOL) and the Department of Justice (DOJ).

C. What is the legal authority?

American Indian Trust Fund Management Reform Act of 1994 (Pub. L. 103-412), 108 Stat.; 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, 161(a), 162(a), 4011, 4043(b)(2)(B).

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*

The PIA was modified to correlate with the System of Records Notice (SORN). The SORN was amended to update location information, routine uses, categories of records, and other entities/sources outside the DOI that information may be shared with. The new SORN also combines the Interior, OS-11, ART SORN with the Interior, OS-02 Individual Indian Money (IIM) Trust Funds SORN into one SORN (January, 2015).

E. Is this information system registered in CSAM?

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

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

010-000000703, ART SSP (07/21/2015)

☐ 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: *List Privacy Act SORN Identifier(s)*

OS-02, Individual Indian Money (IIM) Trust Funds

☐ No

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

☒ Yes: *Describe*

OMB #1035-0004 Trust Funds for Tribal and Individual Indians, 25 Part 115, Expiration December 31, 2020.

☐ No

Section 2. Summary of System Data

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

☒ Name	☒ Religious Preference	☒ Social Security Number (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	☒ Home Telephone Number
☐ Biometrics Information	☒ Credit Card Number	☒ Child or Dependent
☒ Other Names Used	☒ Law Enforcement	☒ Employment Information
☒ Truncated SSN	☒ Education Information	☒ Military Status/Service
☐ Legal Status	☒ Emergency Contact	☒ Mailing/Home Address
☒ Place of Birth	☒ Driver's License	☒ Race/Ethnicity

☒ Other: *Specify the PII collected.*

Date of death if applicable, Tribal affiliation, blood quantum, taxpayer identification number, or contact information for individuals who may know the whereabouts of unknown locations of beneficiaries.

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: *Describe*

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
☒ Other: *Describe*
Requests to third parties may be made if there is an absence of relevant federally available documentation. These inquiries may extend to any entity that may have been involved in a transaction involving Indian Trust resources (e.g., an oil company may have leased the land from an individual or Tribe.)

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

The "Personally Identifiable Information (PII)" data collected directly support OHTA's mission to plan and direct the historical accounting of IIM and tribal accounts and to support DOI and DOJ in litigation. In response to discovery requests including requests for production, requests for Admissions, and interrogatories, OHTA provides documents and data from the ART.

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.*

OST may review information from the ART in preparation of depositions in litigation. OST may also use information from the ART to respond to questions from the SOL and DOJ.

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

The Bureau of Indian Affairs (BIA) to analyze historical collection, distribution, and disbursement of income from Indian Trust land and other revenue sources, and to provide historical statements of accounts to account holders of the IIM and Tribal Trust Funds. SOL uses information from the ART to respond to litigation discovery requests, responds to questions that arise during litigation and settlement discussions.

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

DOJ to analyze historical collection, distribution, and disbursement of income from Indian Trust land and other revenue sources, and to provide historical statements of accounts to account holders of IIM and Tribal Trust Funds.

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

Various local, state, and Tribal entities to analyze historical collection, distribution, and disbursement of income from Indian Trust land and other revenue sources, and to provide historical statements of accounts to account holders of the IIM and Tribal Trust Funds.

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

Contractors under direct contract with OHTA to provide support to the ART System.

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

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: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

None of the data in ART is provided by 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

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

Data is retrieved through ART using Structured Query Language (SQL) queries of various data fields such as, account name, account number, tribal code, etc.

I. Will reports be produced on individuals?

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

The Court, legal teams, DOJ, SOL, & OST for court mandated reports. OST/BIA Managers will grant access to reports to authorized employees for conducting business functions.

☐ No

Section 3. Attributes of System Data

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

Quality Control (QC) procedures from OHTA contractors. When documents are imaged and added to the ART, the OHTA contractor reviews the images to make sure that the image is clear and that all the coded fields match the actual document. When data is added to the ART, data validation is performed to ensure that the account numbers are correct, that the number of transactions is accurate, and to confirm the updating of any records. However, the majority of the information comes from DOI records.

B. How will data be checked for completeness?

QC procedures from OHTA contractors check the completeness of any new information. However, the majority of information comes from DOI records and the completeness there is monitored by the office or bureau.

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

Updates to the database occur on a periodic basis; information is collected from other OST systems; the changes provide updated files for the database. The ART is largely historical or point in time, the system is not intended to maintain current information. The ART does not provide data to any other data stores that would be affected by data not being current.

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

The database maintains historical information that will provide the government information on tribes/individuals. There are various record series applicable to the records associated with ART that are covered by the Indian Affairs Records Schedule (IARS); the electronic records schedule for ART is maintained in accordance with the electronic records schedule, TR-9901-P, ART, approved on 9/28/2006, National Archives and Records Administration (NARA) Job #N1-075-06-08.

Retention periods for records generated by ART vary according to OST functions and specific subject matter, and are retained in accordance with the applicable records retention schedules, as approved by the NARA. Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor.

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

Records associated with the ART follow the applicable IARS for the appropriate record type. In accordance with the IARS disposition instructions, records are maintained in the offices for the designated years after records have become inactive (cut-off); after cut-off, records are retired to the American Indian Records Repository (AIRR), Federal Records Center (FRC) for Indian Trust records. Electronic records: Inputs, master Data Files (history file and current data file), Outputs and Documentation follow the IARS for the appropriate record type. All data records are permanent files where a duplicate copy of the data is transferred to the National Archives in accordance with NARA regulations currently cited in 36 CFR 1228.270.

The electronic records schedule for ART is maintained in accordance with the electronic records schedule, TR-9901-P, ART, approved on 9/28/2006, NARA Job #N1-075-06-08. Retention is permanent. Create duplicate copy of the data off-line and transferred to the National Archives at the end of every three fiscal years in accordance with NARA regulations, such as those currently cited in 36 CFR 1228.270, and related NARA instructions and guidance. Subsequent legal transfer of the records to the National Archives of the United States will be jointly agreed to between DOI and NARA.

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.

All contractors handling the information have a contract with proper non-disclosure clauses and have had at least Low Risk Security Investigations on project staff. The ART contains individual and Tribal account information. The data is protected as access is

granter per user based upon need following the proper security training and non-disclosure agreements. The ART is only accessible while on the DOI Network.

There are risks to the privacy of individuals due to the Personally Identifiable Information (PII) contained in the system related to individual and tribal account information.

The use of DOI information technology (IT) systems is conducted in accordance with the appropriate DOI use policy. OST IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include 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. 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. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign OST Rules of Behavior.

In order to prevent adverse effects to individuals and mitigate the risk for exposing PII contained in the system, OST ensures proper safeguards are in place in accordance with 43 CFR 2.226. Access to sensitive PII is restricted to authorized personnel only who have a need to access the records in the performance of their official duties. Computerized records containing sensitive PII are protected by following the National Institute of Standards and Technology (NIST) standards that comply with the Privacy Act of 1974 (as amended), Paperwork Reduction Act, Federal Information Security Act of 2002, and the Federal Information Processing Standards (FIPPS) 199, Standards for Security Categorization of Federal Information and Information Systems. 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. Authorized personnel and contractors sign a network rules of behavior form, are trained and required to follow established internal security protocols, and must complete the annual Federal Information Systems Security Awareness + Privacy and Records Management (FISSA+) courses. Contract employees are monitored by their Contracting Officer's Technical Representative and OST 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: *Explanation*

The data are absolutely relevant and necessary to the purpose and success of the system and the overall mission of OHTA. OHTA provides litigation support for DOI SOL, and DOJ. In order to support litigation, OHTA uses the ART to provide documents and data and to respond to questions.

☐ 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?

Any new data that is added is quality controlled or reviewed by OHTA Contractors.

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?

Access to the ART is restricted by the role the individual has in working with the data. There are three levels of system access for the ART application; Staff, Supervisor, and Management. Staff – can only perform functions that create reconciled transactions. Supervisor – can review work performed by Staff or Supervisors, approve groups, and complete administrator functions such as user account profiles creation. Management - can review work performed by staff, Supervisors, Management, approve groups and batches, and complete administrator functions such as account profiles creation. Access is requested from OST, using the System Access Request Form, with a specific level of access.

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?*

The appropriate clauses are included in all contracts. Contractors are involved with the maintenance and operation of the system. FAR contract Clauses, Privacy Act Notification of 5 U.S.C. 552a are included by reference in the agreement with the contractor.

☐ 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?

The audit logs capture who was on the system, the date, and time stamps.

Access to the ART 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. Authorized users are trained and required to follow established internal security protocols, must complete all security, privacy, and records management training, and sign the OST Rules of Behavior. Contract employees with access to the system are monitored by the Contracting Officer and OST Associate Chief Information System Security Officer.

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

Access to the ART is restricted by the role the individual has in working with the data.

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 (create,

update, delete, view, assign permissions) and is restricted utilizing role-based access. Authorized users are trained and required to follow established internal security protocols, and must complete all security, privacy, and records management training and sign the OST Rules of Behavior. Contract employees with access to the system are monitored by the Contracting Officer and OST Associate Chief Information Security Officer.

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 System Owner and OST's Information Assurance (IA) team have the responsibility for addressing any privacy risks and ensuring proper safeguards are in place to protect employees and individuals covered by the system. The System Owner and System Manager are responsible for oversight and management of ART security and privacy controls, and for ensuring to the greatest possible extent that OST data is properly managed and that all access to OST data has been granted in a secure manner. The System Owner and System Manager are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of sensitive PII is reported to the Associated Privacy Officer within 1-hour of discovery in accordance with Federal Policy and established procedures.

The System Manager is the official with administrative responsibility for managing and protecting Privacy Act records, whether in electronic or paper format, and for meeting the requirements of the Privacy Act and the published SORN; and responsible for compliance with the 383 DM Chapters 1-13, and DOI Privacy Act Regulations at 43 CFR Part 2.

IA is responsible for ensuring proper use of the system and data.

The Associate Privacy Officer is responsible for ensuring compliance with Federal privacy laws and policies; implements privacy policy, provides guidance, evaluates OST programs, systems and initiatives for potential privacy implications, and provides strategies to mitigate or reduce privacy risk; collaborates with OST program managers, Information System Owners, and IA to ensure privacy considerations are addressed when planning, developing or updating programs, systems or initiatives in order to protect individual privacy and ensure compliance with applicable privacy laws and regulations; and reviewing privacy controls to ensure OST analyzes the privacy risks to meet Federal privacy requirements and demonstrate compliance.

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 OST's IA team are responsible for ensuring proper use of the system and data. The System Owner and System Manager are responsible for oversight and management of ART security and privacy controls, and for ensuring to the greatest possible extent that OST data is properly managed and that all access to OST data has been granted in a secure manner. The System Owner and System Manager are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of sensitive PII is reported to the Associate Privacy Officer within 1-hour of discovery in accordance with Federal Policy and established procedures.

The System Manager is the official with administrative responsibility for managing and protecting Privacy Act records, whether in electronic or paper format, and for meeting the requirements of the Privacy Act and the published SORN; and responsible for compliance with the 383 DM Chapters 1-13, and DOI Privacy Act Regulations at 43 CFR Part 2.

IA is responsible for ensuring proper use of the system and data.

The Associate Privacy Officer is responsible for ensuring compliance with Federal privacy laws and policies; implements privacy policy, provides guidance, evaluates OST programs, systems, and initiative for potential privacy implications, and provides strategies to mitigate or reduce privacy risk; collaborates with OST program managers, Information System Owners, and IA to ensure privacy considerations are addressed when planning, developing or updating programs, systems or initiatives in order to protect individual privacy and ensure compliance with applicable privacy laws and regulations; and reviewing privacy controls to ensure OST analyzes the privacy risks to meet Federal privacy requirements and demonstrate compliance.