U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires Privacy Impact Assessments (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: Trust Evaluation System (TES)
Bureau/Office: Office of the Special Trustee for American Indians (OST), Program Management, Office of Trust Review and Audit (OTRA)
Date: April 21, 2017
Point of Contact:
Name: Elizabeth Wells-Shollenberger
Title: Director, OTRA
Email: elizabeth_wellsshollenberger@ost.doi.gov
Phone: (505) 816-1286
Address: 4400 Masthead St. NE, Albuquerque, New Mexico, 87109

Section 1. General System Information

A. Is a full PIA required?

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

☐ No: *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 Trust Evaluation System (TES) is a web-based software application that is utilized by the OST, Office of Trust Review and Audit (OTRA) for purposes of conducting trust evaluations. These evaluations are critical work performed on behalf of the Secretary of the Interior and the Special Trustee for American Indians to ensure tribes and the Bureau of Indian Affairs (BIA) are in compliance with federal regulations and fiduciary trust standards, as defined by federal laws. The TES will be used to collect data and documentation from tribes and the BIA to evaluate their compliance with federal regulations, statutes, and policies in the management of Indian trust programs. Tribes and the BIA will interactively participate in the trust evaluation process by answering compliance questions, uploading documentation and submitting data to OTRA, via the TES. OTRA auditors will retrieve the data and complete the evaluation. The auditors will also complete all work assignments within the TES (i.e., work papers and develop reports). Documentation collected, will include, uploaded and scanned documents which may contain the names of tribes or trust beneficiaries associated with the ownership of trust assets, leases, court orders, or other trust related transactions and documentation. TES automates the communication flow between OTRA auditors, tribes, and the BIA, allowing for gains in time efficiencies and timely trust evaluation feedback. The TES also enables efficiencies gained in the corrective action tracking process, and timely resolution of deficiencies. The use of the data contained in the TES will be used to perform administrative and mission related trust evaluation functions which also includes evaluation management and risk planning.

Currently, OTRA utilizes the audit software management solution "Auto Audit" (AA). AA is a Commercial Off the Shelf (COTS) proprietary software application published by Thomson Reuters. AA allows OTRA to create, store and manage all audit documentation electronically. AA currently contains some personal identifiable information on trust transaction documents. The AA system currently has employee information such as email addresses, positions, titles and phone numbers. OTRA creates audit case files, collects tribal and BIA data, reports and copies of source documentation. OTRA will transition all electronic case files from AA to TES once the TES is fully developed. TES will need document management capability, storage of case files, and electronic records scheduling. Users (Federal Employees and Tribes) will access TES through a secured web browser through the use of computers and laptop devices. Users will upload text documentation only.

C. What is the legal authority?

The American Indian Trust Fund Management Reform Act of 1994 (P.L. 103-412), 108 Stat. 4239, 25 U.S.C. 4043; Tribal Self Governance Act of 1994 (25 U.S.C 458cc(d)); 25 CFR 1000.350 (Trust Evaluations); Paperwork Reduction Act of 1995; Government Performance and Results Act of 1993 (P.L. 103-62); OMB Circular A-130, Management of

Federal Information Resources; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

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?
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*
010-000001874

☐ 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*

OTRA is currently working with the DOI Information Clearance Collection Office for OMB approval. A OMB Control Number will be included after OMB approval is acquired.

☐ 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	☐ 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	☐ Driver's License	☒ Race/Ethnicity

☐ Other: *Specify the PII collected.*

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*

The system will not collect new information (Personally Identifiable Information, PII) but may contain PII in the scanned copies (not originals) of leases, probates, use and distributions plans, court ordered documentation, trust system documentation, and reports from other sources, i.e., Trust Funds Accounting System (TFAS), Bureau of Indian Affairs (BIA) Trust Asset and Accounting Management System (TAAMS), Pro Trac (Asset/Ownership data). Scanned documents may also contain pricing information for individual securities from outside vendors,

beneficiary information regarding individuals' locations whose whereabouts are currently unknown from private entities, address information from the U.S. Postal Service and other entities that conduct trust-related business with DOI.

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

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

The intended use of the data (PII) contained in the system will be to perform administrative and mission critical functions related to the planning of evaluations of trust programs, functions, and activities managed/administered by tribes or the BIA.

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:*

Data/reports may be shared within OST to upper management to note compliance, or lack thereof, to trust requirements.

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

Data/reports may be shared with the Bureau of Indian Affairs (BIA), Office of Self-Governance (OSG), and/or appropriate government and tribal personnel to communicate audit results, issues and coordinate corrective actions. Data may also be shared with the Office of Inspector General and Governmental Accounting Office in response to, audits, evaluations and inspections by special request.

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

Data/reports may be shared with Tribes/Consortiums that compact trust programs to note compliance, or lack thereof, to trust requirements.

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

Data may be shared with the Contractor that performs the Annual Trust Funds Audit (i.e. Independent Audit of the Financial Statements for Tribal and Other Trust Funds and Individual Indian Monies Trust Funds).

☐ 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:*

OTRA does not have direct contact with individuals members of the public or indian individuals. OTRA performs trust evaluations on behalf of the Secretary (25 CFR Part 1000.350) and the Special Trustee for American Indians (American Indian Trust Fund Management Reform Act of 1994, P.L. 103-412).

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 be retrieved by a personal identifier which can be either the name of a Tribe/Consortium, location, Region, Agency name, Auditor name, and/or an OTRA report number associated with the audit (i.e., OTRA-17-000T).

I. Will reports be produced on individuals?

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

☒ No

Reports are not produced on individuals. The tribes, federal employees and auditors report on the performance of trust programs, services, functions or activities. OST and BIA managers may generate and/or will have access to the reports. The reports are produced to report on fiduciary trust performance of tribes and the BIA. Trust evaluation data (i.e. locations, milestone dates, hours, reports issuance dates, types of findings, and corrective action tracking milestone due dates) is collected in the process of performing the trust evaluations.

Section 3. Attributes of System Data

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

The data collected from sources other than DOI will be verified with tribes and the BIA. Tribes and the BIA that submit the data and information will be responsible for the accuracy of the data provided.

B. How will data be checked for completeness?

The entities evaluated (i.e. tribes and the BIA) are responsible for ensuring the completeness of data contained within the system (paper and electronic). OTRA performs a reconciliation of automated reports and hard copy or source documentation as part of the internal verification process. Also, it is the responsibility of the individual (tribal or BIA) entering the data into the TES to check for completeness of the data. Those individuals are responsible for ensuring the information is correct by verifying the information with appropriate points of contact within their respective entities (i.e. tribe or BIA).

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

No current data will be collected. The system will capture and store historical documentary evidence collected by scanned documents from the tribes and the BIA. It is the responsibility of the individual entering data into the TES to check for the currency of the data. Data is only collected and used by employees and contractors for authorized purposes.

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

Trust evaluation records are maintained in accordance with the OST Indian Affairs Records

Schedule (IARS) TR-6005-P2, Assessment Files which was approved by the National Archives and Records Administration (NARA) (Job # N1-075-07-17, Approved 5/17/2007). The Files cover records related to correspondence, reports, questionnaires, uploaded trust transactions and documentation, action copies of trust examination findings, and other records that identify program internal control weaknesses, and corrective actions and supporting documentation taken to resolve. Currently, the disposition for these records is permanent with a cut-off date of at the end of the fiscal year that the case file is closed. The retention period following, is 2 years from the cut-off date.

The records will be retained in accordance with the applicable Department or OST IARS series and item. If the records are determined as "unscheduled", OTRA will work with the Office of Trust Records (OTR) and the system will go through a scheduling and approval process through NARA. Records may also be 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?

OTRA follows the OST Indian Affairs Records Management Manual (IARMM) for all procedures required for Indian trust data, source documents, hard copy records and electronic records disposition requirements at the end of the disposition schedule. Trust examination, Evaluation and Assessment files are dispensed in accordance with the time periods and procedures in the IARMM. All OTRA records are shipped and stored permanently at the American Indian Records Repository in Lenexa, Kansas, at the end of the 2 year retention period for the case files, or in accordance with current records schedules.

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 use of TES is conducted in accordance with the appropriate DOI use policy. 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. OST employees and contractors are required to complete security and privacy awareness training and as authorized users who manage, use, or operate TES 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 (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. Data is protected through user identification, passwords, database permissions, and software controls.

The 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. Contract employees are monitored by their Contracting Officer 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 use of the data contained in the system are relevant and necessary to perform administrative and mission critical functions, specifically to perform trust evaluations as required by federal regulations and public law.

☐ 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 data is reconciled with hard copy source documents and system data or reports to determine relevance and accuracy. The system does not derive new data about an individual.

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*
Upon request of a tribe(s) that have compacted trust functions and which has been evaluated, the tribe would be authorized view access to the evaluation information that pertains ONLY to their (respective) evaluation information.

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

All authorized users have access to view account information. Access to TES 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. 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 Representative and OST ACISO.

The System Owner, system administrator, and supervisor determines user access based on the role and duties of the employee (contractor). Access to all data is restricted to authorized personnel based on official need-to-know.

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

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

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

☐ No

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

☐ Yes. *Explanation*

☒ No

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

☐ Yes.

☒ No

TES stores audit assessment and evaluation historical data. TES does not allow for routine file maintenance functions, such as, to correct addresses, names, or to identify, locate and monitor individuals.

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

TES does not monitor individuals.

Access to TES 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 Representative and ACISO.

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

TES does not monitor individuals.

Access to TES 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 Representative and ACISO.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(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 is responsible for implementing the legal information resources management requirements including Privacy, Security, Records Management, Freedom of Information Act, and data administration. The Associate Privacy Officer (APO) is responsible for addressing Privacy Act complaints. The System Manager and APO are responsible for responding to and processing requests for access or amendment of records.

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 a 43 CFR Part 2.

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 System Manager are responsible for oversight and management of TES 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. They are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of sensitive PII be reported to: 1) OST Security at ost_security@ost.doi.gov , 2) Immediate Supervisor, and 3) APO at Veronica_Herkshan@ost.doi.gov 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, for meeting the requirements of the Privacy Act and the published SORN; and is responsible for compliance with the 383 DM Chapters 1-13, and DOI Privacy Act Regulations at 43 CFR Part 2.

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

The APO 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 IT Security 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.

Section 5. Review and Approval

Information System Owner

Name: John White
Title: Deputy Special Trustee – Program Management
Bureau/Office: OST, Office of Trust Review and Audit
Phone: (505) 816-1328 Email: John_White@ost.doi.gov

Signature: _____ Date: _____

Associate Chief Information Security Officer

Name: Larry Sorensen
Title: Acting Associate Chief Information Security Officer
Bureau/Office: OST, Office of Information Resources, Information Assurance
Phone: (505) 816-1249 Email: Larry_Sorensen@ost.doi.gov

Signature: _____ Date: _____

Associate Privacy Officer
Name: Veronica Herkshan
Title: Acting Associate Privacy Officer
Bureau/Office: OST, Office of Information Resources
Phone: (505) 816-1645 Email: Veronica_Herkshan@ost.doi.gov

Signature: _____ Date: _____

Reviewing Official

Name: Teri Barnett
Title: Departmental Privacy Officer
Bureau/Office: DOI, Office of the Chief Information Officer
Phone: (202) 208-1943 Email: Teri_Barnett@ios.doi.gov

Signature: _____ Date: _____