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: Trust Asset and Accounting Management System (TAAMS)
Bureau/Office: Bureau of Indian Affairs, Office of Trust Services (Division of Probate Services/Special Projects)
Date: September 29, 2021

Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Road NW, Albuquerque, New Mexico 87104

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 Department of the Interior (DOI), Bureau of Indian Affairs (BIA) manages 48.7 million acres of tribally owned land, 6 million acres of Federally owned land, and approximately 181,000 acres of Federally owned land held in Trust status. The BIA is responsible for managing over 125,000 leases, use permits, land sales, and other encumbrances, as well as interest on deposited funds. Approximately $650 million is collected annually for approximately 163,000 Individual Indian Money (IIM) accounts.

The Trust Asset and Accounting Management System (TAAMS) is the DOI's integrated land management system. TAAMS is a contractor maintained and contractor operated major application. It is the system of record for title and land ownership data for land held in trust by the DOI for Tribes, American Indians, and Alaska Natives. The system manages the leasing process including the invoicing and distribution of income to the Department's beneficiaries on the land held in trust for Tribes, American Indians, and Alaska Natives. The system also manages the Osage Headright Rights and facilitates the beneficiary distribution to Head Right Owners.

TAAMS allows users to access, create, and modify records in the database for land ownership, contracts and leases, and beneficial owners. TAAMS currently consists of modules including Conveyance, Legal, Title Tract, Surface, Mineral, Right-of-Way, Range, Forestry, Name and Address, Reports, Receivable, Invoicing/Funds/Payments, System Maintenance, and Land Buy Back, Commercial Leasing, Inquiry Case.

TAAMS data is not shared with any other systems outside the DOI. The data is shared between the Trust Fund Accounting System (TFAS) and TAAMS through a manual process. TFAS is owned by the Bureau of Trust Funds Administration (BTFA) (previously the Office of the Special Trustee for American Indians). TFAS provides data about individuals who receive payments from BTFA for natural resources, such as gas and oil that is produced on their land. The TFAS PIA can be viewed at: tfas-innovest-pia.pdf

Natural resource revenue data is retrieved from the Mineral Revenue Management Support System (MRMSS) through a manual process for use within TAAMS. MRMSS is managed by the Office of Natural Resources and Reporting (ONRR) which provides revenue management services for mineral leases on Indian lands. The MRMSS PIA can be viewed at: https://www.doi.gov/sites/doi.gov/files/mrmss-pia-08052019.pdf

TAAMS will interface through a secure connection with the DOI Appraisal and Valuation Services Office (AVSO), Interior Valuation Information System (IVIS). IVIS is a case management application used by the DOI Office of the Secretary, AVSO. IVIS is an electronic real estate appraisal tracking system that is used to request appraisals, assign requests to appraisers, and notify users of assignment status. System integration with TAAMS during the appraisal request process ensures data quality, data consistency, and compliance with metrics regarding appraisal processing time. The information collected from TAAMS consists of land ownership or contact information. The IVIS PIA can be viewed at: https://www.doi.gov/sites/doi.gov/files/uploads/ivis_pia_09282017.pdf

C. What is the legal authority?

American Indian Trust Fund Management Reform Act of 1994 (Pub. L. 103-412); The Act of March 3, 1921 (Pub. L. 66-359); Self-Governance Compacts (Pub. L. 93-638); American Indian Probate Reform Act of 2004 (Pub. L. 108–374); Indian Land Consolidation Act (25 U.S.C. 2201 et seq.); American Indian Trust Fund Management Reform (25 U.S.C. 42); 25 U.S.C. 5, 12, 116, 117(a)(b)(c), 118-121, 151, 159, 161(a), 162(a), 163, 392, 393, 406, 407, 413, 415, 2106, 4001-4061, 4011, 4043(b)(2)(B), 5363(d)(1); 25 USC 4041, 25 USC §5363 (d) (1), 43 USC 1601; 25 CFR 1000.350, 25 CFR 1000.355, 25 CFR 1000.365; 25 CFR Part 15, Probate of Indian Estates, Except for Members of the Osage Nation and the Five Civilized Tribes; 25 CFR Part 117, Deposit and Expenditure of Individual Funds of Members of the Osage Tribe of Indians who do

not have Certificates of Competency; 25 CFR Part 150, Land Records and Title Documents; 25 CFR Part 151, Land Acquisitions; 25 CFR Part 152, Issuance of Patents in Fee, Certificates of Competency, Removal of Restrictions, and Sale of Certain Indian Lands; 25 CFR Part 161, Navajo Partitioned Lands Grazing Permits; 25 CFR Part 162, Leases and Permits; 25 CFR Part 166, Grazing Permits; 25 CFR Part 167, Navajo Grazing Regulations; 25 CFR Part 1000, Annual Funding Agreements Under the Tribal Self-Government Act Amendments to the Indian Self-Determination and Education Act, Subpart O—Trust Evaluation Review, §§ 1000.350, 1000.355, 1000.365; 43 CFR Part 4, Department Hearings and Appeals Procedures.

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 Code: 010-000000077, Trust Asset Accounting Management System (TAAMS), 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.*
None	Not Applicable	No	Not Applicable

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 following system of records notices may be viewed at https://www.doi.gov/privacy/sorn.

- BIA-04, Trust Asset Accounting Management System (TAAMS), 79 FR 68292 (November 14, 2014)
- OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, (March 25, 2016), for information related to lease ownership of the Individual Indian Mineral Interest Owner.
- OS-02, Individual Indian Money (IIM) Trust Funds, 80 FR 1043 (January 8, 2015), for information related to land consolidation activities.

☐ No

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

☒ Yes: *Describe*

- OMB Control No. 1076-0100 - Acquisition of Trust Land, 25 CFR 151, Expires 01/31/2024
- OMB Control No. 1076-0104 - Federal Acknowledgment as an Indian Tribe, 25 CFR 82 & 83, Expires 12/31/2023
- OMB Control No. 1076-0155 - Leases and Permits, 25 CFR 162, Expires 11/30/2022
- OMB Control No. 1076-0157 - Grazing Permits, 25 CFR 166, Expires 03/31/2023
- OMB Control No. 1076-0157 - Authority to Grant Grazing Privileges on Allotted Lands, Form 5-5525, OMB Control No. 1076-0157, Expires 03/31/2023
- OMB Control No. 1076-0181, 25 CFR 169, Rights-of-Way on Indian Land, Expires 06/30/2023

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Gender
☒ Place of Birth
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Other Names Used
☒ Mailing/Home Address
☒ Social Security Number (SSN)
☒ Spouse Information
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Other: Social Security number (SSN) for each Indian or non-Indian landowner. Not all records on individuals include SSN. The SSN is used to ensure accurate identification of an individual because people may have the same name and date of birth. Accurate identification is necessary as is providing a SSN to the U.S. Department of Justice and the Department of the Treasury when necessary to collect program debts or report taxable income as required by law. Information about parents of landowners for identification purposes; name, address, phone number and Federal tax identification number of each person or entity who has a permit, lease, contract, right-of-way, or other legal instrument approved by the Secretary of the Interior that allows such entity to use the trust or restricted land, or to extract renewable or nonrenewable resources from such land; name, address, phone number and Federal taxpayer identification number of any company that has a permit, lease, contract, right-of-way or other legal instrument approved by the Secretary of the Interior that allows such company to use the trust or restricted land or to extract renewable or nonrenewable resources from such land; trust income collected and distributed for such permit, lease, contract, right-of-way or other legal instrument; official correspondence, appraisals, maps, purchase offers, and other documents related to land consolidation efforts or other program activities that may include name, address, email address, phone number, age, date of birth, SSN, Tribal enrollment number, BIA identification number, land ownership interests in restricted or fractioned lands, and other information related to these program activities.

Tax Identification Number (TIN) for businesses. TAAMS may also contain records concerning private businesses and financial institutions that are not subject to the Privacy Act, as well as data on a small proportion of sole proprietors, which is covered by the Privacy Act. Information collected is limited to private businesses and financial institutions that have a permit, lease, contract, right-of-way, or other legal instrument approved by the Secretary of the Interior that allows them to use trust or restricted land, or to extract resources from the trust or restricted land. Records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information. TAAMS may also contain information about businesses by sole proprietors who operate under their own names, and information concerning these sole proprietors could include name, business address, and business mailing address, business telephone numbers, and business email address. The personal and contact information in the system is largely available through public sources.

TAAMS data is not shared with any other systems outside the DOI; however, there is a data exchange between TAAMS and TFAS, which is owned by the BTFA. TFAS provides TAAMS with files containing names and addresses of individuals who receive payments from BTFA for natural resources, such as gas and oil that is produced on their land.

Authorized ONRR users have access to TAAMS, the system of record for title and land resource management of Indian Trust and Restricted Land within DOI and BIA, to manually retrieve data regarding lease ownership of the Individual Indian Mineral Interest Owner (IIMIO), which is used to verify royalty payments to Tribes and IIMIO owners.

This system may also contain information regarding DOI and BIA employees and officials who are acting in their official capacity to administer program activities, or who are involved in land title and resource management functions, which is limited to system authentication and work contact information.

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: Indians, private, financial, or business institutions and entities. PII is added to TAAMS via a secure interface from the TFAS. TFAS is the system of record for the financial activity transacted by TAAMS.

TAAMS interfaces with the BTFA TFAS, which provides a data file upon which distribution of funds is made and sharing and updating data on revenue distribution between the systems. Files provided from TFAS to TAAMS contains names, addresses, and other personal data about individuals who have IIM accounts in TFAS.

TAAMS interfaces with the Office of Natural Resources and Reporting (ONRR), Minerals Revenue Management Support System (MRMSS) which provides revenue management services for mineral leases on Indian lands. The MRMSS provides natural resource revenue data to be distributed to landowners within the TAAMS system.

Records in the system may be obtained from (a) DOI Bureaus and Offices including BIA, BTFA, ONRR, BLM, Office of Hearings and Appeals, and other Bureaus and Office programs; (b) other Federal, state and local agencies; (c) Tribal offices if the title or realty function is contracted or compacted under the Indian Self Determination and Education Assistance Act, Public Law 93–638; (d) Courts of competent jurisdiction, including tribal courts; (e) private, financial and business institutions, and entities; and (f) correspondents, participants, beneficiaries, land owners, and members of the public.

The Natural Resource Conservation Service (NRCS) and Farm Service Agency (FSA) of the United States Department of Agriculture (USDA) may provide name and address of producers via a report to BIA to assist in the distribution of funds, to the appropriate BIA authority when a default involves a security interest in Tribal allotted or trust land and information concerning default on a loan repayment per 42 U.S.C. 1207 et. seq., and to determine eligibility of a trust parcel, or the beneficial owners or authorized users of a trust parcel for participation in USDA programs. Information on USDA's sharing information with BIA can be seen at:

- USDA/FSA-2, Farm Records File
- USDA/FSA-14, Applicant/Borrower

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: Names, Addresses, and other contact data are provided by the TFAS. TAAMS uses a Secure File Transfer Protocol/Transport Layer Security (SFTP) to transfer trust data files from TFAS. This file could then update an owner's name, TFAS account status/type or financial address in TAAMS.

Name, address, and contact data on individuals who receive payments for natural resources, such as gas and oil, produced on their land is provided by the MRMSS. MRMSS uses SFTP to transfer data to TAAMS.

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

Data collected in TAAMS is used for the management of Indian trust lands for the benefit of Trust landowner beneficiaries. TAAMS is the system of record for title and land resource management of Indian Trust and Restricted Land within the DOI and the BIA. TAAMS provides DOI and Tribal Users access to trust asset data and trust asset management tools to create, modify and maintain records for land ownership, contracts, leases, and beneficial owners. TAAMS functionalities include title, leasing, accounting, and reporting modules to maintain and track land title documents, contracts, right of way, revenue distributions, invoicing, collections, acquisitions, legal details relating to land transactions, receipt and distribution of trust funds, title status, owner inventory, chain of title, and oil and gas royalty distributions. TAAMS also supports DOI land consolidation activities, and provides a secure interface to TFAS, an

accounting system used to meet DOI's fiduciary trust responsibilities for managing the receipt, investment, and disbursement of monies held in trust for individual Indians, Alaskan Natives, and Tribes.

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 collected in TAAMS is used within BIA for the management of Indian trust lands for the benefit of Indian beneficiaries. Contracts, leases, right of ways, and other income producing actions are captured in TAAMS. Individual land interests are maintained in TAAMS allowing for the distribution of income to individual Indian beneficiaries based on ownership shares.

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

Data is shared with BTFA to use ownership and income producing actions in TAAMS to determine income distribution to individual Indian beneficiaries. The MRMSS shares data with TAAMS to provide information on oil and gas income to be distributed based on individual Indian ownership. BLM also uses TAAMS data to provide Indian beneficiaries services.

DOI Appraisal and Valuation Services Office's IVIS will pull property data from TAAMS, consisting of tract legal description, tract information and lease information.

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

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

U.S. Department of Justice, a court of an adjudicative or other administrative body, a party in litigation before a court or administrative body. The Department of the Treasury to recover debts owed to the United States.

Information may be shared with other Federal agencies when authorized or required by law, as outlined in the routine uses in BIA-04, Trust Asset Accounting Management System (TAAMS), 79 FR 68292 (November 14, 2014), which may be viewed at: https://www.doi.gov/privacy/sorn.

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

Information may be shared with Indian Tribes that exercise jurisdiction over the lands where a parcel is located. With State, territorial, and local governments and tribal organizations to provide information needed in the performance of its duties or in response to a court order and/or discovery purposes related to litigation when the disclosure is compatible with the purpose for which the records were compiled.

Information may be shared with Indian Tribes entering a contract or compacts of real estate or title functions under the Indian Self Determination and Education Assistance Act, as amended.

Information may be shared with Indian Tribes (including tribal employees) that (1) operate, or are eligible to operate, land consolidation activities on behalf of the Department of the Interior (DOI), (2) agree to nondisclosure, and (3) submit a request in writing, upon a determination by the Department that such activities shall occur on the tribe's reservation and when the

information relates to owners of fractionated land. Information disclosed may include but not be limited to the following: (a) Contact information; (b) Relevant personal characteristics of the owner, including age, tribal membership, and whether alive or deceased; (c) Details regarding the type of ownership, such as the type of interest and whether the interest is purchasable; and (d) Status information on or about transactions, such as whether an offer has been sent, accepted, or rejected, and whether the owner is a willing seller.

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

Information may be shared with a DOI contractor and their authorized employees that perform services requiring access to records on DOI's behalf to carry out the purposes of the TAAMS.

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

Indian Affairs may share information to a Congressional Office in response to an inquiry concerning an individual whose information is contained in TAAMS or records related to a parcel of land maintained in the system. And Consumer Reporting Agencies may receive information pursuant to 5 U.S.C. 552a(b)(12), disclosures may be made to a consumer reporting agency as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) or the Federal Claims Act of 1966 (31 U.S.C. 3701(a)(3).

Information may be shared with any of the following entities or individuals, when the entity or individual makes a written request for names or mailing addresses of owners of any interest in trust or restricted lands, and information on the location of the parcel and the percentage of undivided interest owned by each individual: (i) Other owners of interests in trust or restricted lands within the same reservation; (ii) The tribe that exercises jurisdiction over the land where the parcel is located or any person who is eligible for membership in that tribe; and (iii) Any person that is leasing, using, or consolidating, or is applying to lease, use, or consolidate, such trust or restricted land or the interest in trust or restricted lands.

Information may be shared with third parties when authorized and necessary or required by law, as outlined in the routine uses in BIA-04, Trust Asset Accounting Management System (TAAMS), 79 FR 68292 (November 14, 2014), system of records notice which may be viewed at: https://www.doi.gov/privacy/sorn.

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.*

The information in TAAMS is collected directly from the individual and from transactions affecting land ownership and rights. The information is used to manage land and individual Indian interests to generate income and ensure proper disbursement of income. Response is required to obtain a benefit. Failure to provide necessary information may result in a delay in receiving or denial of a benefit.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

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

A Privacy Act Statement is included on the forms (information collections) provided to beneficiaries. The OMB approved these forms as part of the BIA Information Collections. Each form includes the requisite information on the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this privacy impact assessment and the published BIA-04, Trust Asset Accounting Management System (TAAMS), 79 FR 68292 (November 14, 2014); OS-02, Individual Indian Money (IIM) Trust Funds, 84 FR 44321 (August 23, 2019), and OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207 (March 25, 2016). These SORNS may be viewed at: https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

Information is retrieved by trained individuals with authorized access to TAAMS in the performance of official functions. Records are retrieved using either: (a) an identifier linked to a land parcel; (b) an identifier for a property interest owner, such as name, SSN, tribe, tribal enrollment, or census numbers; or (c) identifiers linked to encumbrances on ownership such as mortgages and rights of ways; search by name, owner identification number, land area codes, parcel or tract identifiers or document identification number are possible. Users with the proper permissions can create customized result sets containing any information in the system.

I. Will reports be produced on individuals?

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

Any data field in TAAMS can be used to generate information in a report format. Although land title records are available to the public in accordance with the American Indian Probate Reform Act (AIPRA), in general the use of information on individual landowners is restricted to those individuals who have a need-to-know in the performance of their official duties. DOI, BIA, and their agents, including TAAMS contractors, and tribes that compact or contract, or enter into cooperative agreements with the DOI use the record to:

(a) Identify ownership interests, including the name of Indian owners, and percentage of interest in Indian lands held in trust or restricted status.
(b) Record land conveyance, encumbrance, and lien transactions.
(c) Determine beneficial rights to the land and resources.

(d) Appropriately manage trust and restricted land and natural resources for the benefit of the Indian landowner.
(e) Provide land statistics in support of budget and management initiatives; and
(f) Answer beneficiary questions regarding land rights.

Audit logs can be used to run reports detailing an individual users' authorized access and actions performed in TFAS. Information collected as a function of monitoring authorized users' may include username, failed attempts, files accessed, and user actions.

☐ No

Section 3. Attributes of System Data

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

TAAMS collects data directly from individuals and from other internal DOI systems. It is the responsibility of the system owners of the internal systems to ensure data maintained is accurate. However, to the maximum extent possible data collected from sources other than DOI records is verified by one of the following: 1) Individuals or Tribes verify that information is accurate; 2) Supporting documentation is required for data verification such as birth certificates, divorce decrees, certificates of death, and signed affidavits; 3) Data entered in TAAMS by BIA is subject to internal system validation based on preprogrammed business rules developed from a process known as Business Process Reengineering (BPR). For example, a date of birth or date of death cannot be in the future. Additionally, validation against internal business rules and existing land trust deeds and records is conducted.

TFAS authorized users use the United States Postal Service Coding Accuracy Support System to evaluate, match, and correct street addresses.

TAAMS authorized users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

B. How will data be checked for completeness?

TAAMS collects data directly from individuals and from other internal DOI systems. It is the responsibility of the system owners of the internal systems to ensure data maintained is complete. The individual is responsible for ensuring the information provided is complete. TFAS uses the national change of address database to validate and supply missing information for addresses.

TAAMS authorized users are responsible for ensuring the completeness of the data associated with their user accounts. Data is checked for completeness during the account creation process.

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

The individual is responsible for ensuring information provided is current. TAAMS collects data from other internal DOI systems, and it is the responsibility of the system owners of these internal systems to ensure data maintained is current.

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the currency of their records.

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

Records are covered by Indian Affairs Records Schedule (IARS) Records Series 2200-Trust Asset and Accounting Management System (TAAMS) and approved for permanent retention under NARA Job Number N1-075-09-008, approved on February 13, 2013. Records are maintained in the office of records for a maximum of 5 years. Records are cut-off at the end of the fiscal year. The records are then retired to the American Indian Records Repository which is a Federal Records Center. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the Department of the Interior (DOI) and NARA.

TAAMS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

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

TAAMS paper and electronic records have a permanent retention and are retired to the American Indian Records Repository (AIRR), which is a Federal Records Center. Subsequent legal transfer of the records to the National Archives of the United States will be jointly agreed to between DOI and NARA. Data disposition follows NARA guidelines and approved Records Schedule for transfer, pre-accession, and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins, and the records management policies and procedures of the BTFA, Office of Trust Records, which is the office that provides records oversight and develops records retention and disposition schedules for the BIA. System administrators dispose of temporary records by shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction) affect individual privacy.

There is a risk to the privacy of individuals due to the volume of sensitive PII collected and maintained in TAAMS. To mitigate the privacy risks, TAAMS has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. TAAMS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information. A System Security and Privacy Plan

documenting required privacy and security controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system has been completed.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access are based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages TAAMS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of TAAMS user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Employees complete privacy training annually which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that TAAMS may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained to provide a service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system

access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, based on the "least privilege" principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. TAAMS meets BIA's information system security requirements, including operational and risk management policies.

There may be a risk associated with maintaining records with accuracy and currency. Information is obtained directly from individuals where possible and from other internal DOI records. Individuals may contact the Trust Beneficiary Call Center, which is a nationwide, toll-free call center that enables beneficiaries to conveniently access information regarding their trust assets, check the status of a trust service, request a disbursement, or an update to their IIM Account, and submit requests for account updates. Individuals may also submit a Privacy Act request or complaint to the TAAMS System Manager or APO as outlined in the BIA-04, Trust Asset Accounting Management System (TAAMS), system of records notice which may be viewed at: https://www.doi.gov/privacy/sorn.

There may also be a risk associated with the accuracy and currency of supporting documentation collected from TFAS and MRMSS. BIA relies on the accuracy and currency of documentation obtained from TFAS and MRMSS, which is the responsibility of the TFAS and MRMSS system owners. BTFA and ONRR have conduct privacy impact assessments on these systems to evaluate the privacy risks and mitigating controls and ensure information provided to BIA for use in TAAMS is authorized. BTFA and ONRR are responsible for the accuracy and currency of information provided to BIA.

There may be a risk associated with the collection of information from other DOI systems. TAAMS collects data from other internal DOI systems and BIA relies on the accuracy and currency of data, which is the responsibility of each system owner. The additional risk of transferring data electronically from one system to another is mitigated by using secure data transfer protocols. For example, the data transfer from TAAMS to IVIS is controlled in both direction by dedicated source and destination addresses using supported secure protocols. All connections are subject to appropriate authentication and end-to-end encryption standards. Additionally, IVIS user accounts are managed by the AVSO IVIS System Administrator and has privileges to add, modify and delete user accounts. All active IVIS users access the system using their Personal Identity Verification card. Bureau managers are responsible for authorizing access to IVIS users. Bureau managers are responsible for reviewing their Bureau's user's accounts and notifying the IVIS System Administrator when no longer needed. The IVIS System Administrator reviews accounts that have not accessed the system in the last 90 days and disables accounts determined to be inactive.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The Division of Probate Services is responsible for managing and disposing of BIA records in TAAMS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. The Division of Probate Services ensures only records needed to support its program, Tribes, and Tribal members is maintained. The Division of Probate Services maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-09-008: Series 2200 – TAAMS. TAAMS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off. Information collected and stored within TAAMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information, including how it will be used, or that their PII is sourced from other DOI internal system such as TFAS and MRMSS. Individuals are notified of the privacy practices through the Privacy Act statements provided on TAAMS forms, this PIA and through the published BIA-04, Trust Asset Accounting Management System (TAAMS), 79 FR 68292 (November 14, 2014); OS-02, Individual Indian Money (IIM) Trust Funds, 84 FR 44321 (August 23, 2019), and OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207 (March 25, 2016), which may be viewed at: https://www.doi.gov/privacy/sorn. These SORNs provide a detailed description of system data elements and how an individual's PII is used.

There may be a risk related to TAAMS being hosted at a non-DOI managed data center by a vendor, or that the vendor may not handle or store information appropriately according to DOI policy. TAAMS is hosted and administered within a DOI-approved data center by a vendor under contract with DOI. The vendor is required to meet all Federal, National Institute of Standards and Technology (NIST), DOI and Indian Affairs, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, security control requirements. They must have an approved authority to operate (ATO) and are assessed as part of the information systems ATO being hosted in the data center. BIA manages system access using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of system user accounts.

In addition to the risk mitigation actions described above, the BIA maintains an audit trail of activity sufficient to reconstruct security relevant events. The BIA follows the 'least privilege' security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles

of separation of duties. Controls over information privacy and security are compliant with NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of TAAMS data is both relevant and necessary to the purpose for which the system was designed. The Department of the Interior (DOI), Bureau of Indian Affairs (BIA) manages 48.7 million acers of tribally owned land, 6 million acres of Federally owned land, and approximately 181,000 acres of Federally owned land held in Trust status. The BIA is responsible for managing over 125,000 leases, use permits, land sales, and other encumbrances, as well as interest on deposited funds. Approximately $650 million is collected annually for approximately 163,000 Individual Indian Money (IIM) accounts. TAAMS was developed to provide an effective and accurate system for managing data on Trust assets associated with Trust land. TAAMS provides comprehensive national Trust information to Indian Affairs and Indian Tribal officials in support of the Agency's Trust management responsibilities.

☐ 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. TAAMS is not intended to be used in any manner that would allow the system to 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: Tribal Users, BTFA Call Center personnel

Users, Contractors, Developers, System Administrators, and BTFA Call Center personnel are given access to TAAMS data on a 'least privilege' bases and a 'need-to-know' to perform official functions. Authorized Tribal users under government compacts or contracts may be granted access to Tribal-specific data. Contractors and developers supporting the system and performing system maintenance and other related activities may have access to the data in the system.

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

Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages TAAMS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of TAAMS user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

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 responsible for designing, developing, and maintaining the system. Federal Acquisition Regulation Security and Privacy Act Clauses and other security and privacy provisions are in the Contract to protect DOI information systems and data. Contractors are

required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The Privacy Act contract clauses listed below were included in the contract. However, all required contract clauses will be included in the next contract update.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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*

The purpose of TAAMS is not to monitor individuals. However, audit logs are maintained on user access to the system, as well as changes to data made by users of the system. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination.

☐ No

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

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Information about landowners and others associated with land transactions(s) are identified only as needed to capture land transactions.

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

TAAMS can audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring. TAAMS System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. TAAMS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users are required to consent to TAAMS Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The TAAMS audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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 (Biometric hand and palm geometry scanners are used at the data center.)
- ☒ 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 Associate Chief Information Officer is the Information System Owner and the official responsible for oversight and management of the TAAMS security and privacy controls and the protection of agency information processed and stored in the TAAMS system. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in TAAMS. These officials and authorized TAAMS personnel are responsible for protecting individual privacy for the information collected, maintained, used, shared, and disposed of in the system, and for meeting the requirements of the Privacy Act. The TAAMS System Manager is responsible for providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with DOI privacy officials.

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 TAAMS Information System Owner and Information System Security Officer are responsible for daily operational oversight and management of the system's security and privacy controls and ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The TAAMS Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and DOI privacy officials within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in consultation with DOI Privacy Officials. All DOI employees and contractors are responsible for safeguarding privacy, reporting any compromise of PII, and complying with Federal and Departmental privacy requirements.