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 Funds Accounting System (TFAS), Innovest
Bureau/Office: Office of the Special Trustee for American Indians (OST), Trust Services
Date: 2/22/2019
Point of Contact: Dianne Moran
Name: Dianne Moran
Title: System Manager, Financial Systems Administrator
Email: dianne_moran@ost.doi.gov
Phone: (505) 816-1060
Address: 4400 Masthead Street 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 Office of the Special Trustee for American Indians (OST) Trust Funds Accounting System (TFAS), Innovest Systems LLC, assists OST in meeting the fiduciary responsibilities set forth in the American Indian Trust Fund Management Reform Act of 1994 including management of

the receipt, investment, disbursement and administration of money held in trust for individual Indians and Alaskan Natives (or their heirs), and Indian Tribes, and ensures timely, accurate, and consistent responses to beneficiary inquiries.

The system also assists the OST in providing litigation support by analyzing and reconciling the historical receipt, distribution, and disbursement of income from individual Indian Money (IIM) and Tribal trust accounts, Indian trust land, and other revenue sources. The system also helps OST improve accountability and management of Indian funds held in trust by the Government; provide trust services and information for Indian trust funds program management; manage beneficiary contact including inquiries and requests regarding their trust assets; provide IIM account status to IIM account holders; locate IIM account holders whose whereabouts are currently unknown; document trust account transaction history and quarterly statements; and transfer electronic data to the Department of the Treasury for the processing of IIM account and Tribal trust fund account payments.

It also supports the Department of the Interior (DOI) land consolidation activities and provides an interface to the Trust Asset and Accounting Management System (TAAMS), a system of records for title and land resource management of Indian trust land within DOI and the Bureau of Indian Affairs (BIA).

This updated TFAS privacy impact assessment (PIA) is being conducted to evaluate risks related to migrating TFAS data to a new vendor hosted by a cloud service provider. The TFAS PIA approved on, March 9, 2017, will remain in effect until the migration to the new vendor is completed and any residual data is disposed of in the legacy system.

C. What is the legal authority?

The American Indian Trust Fund Management Reform Act of 1994 (Pub. L. 103–412, 108 Stat. 4239; 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, 159, 161(a), 162(a); 4011, 4043(b)(2)(B); Pub. L. 93-638 Self-Governance Compacts; 25 U.S.C. 5363(d)(1); 25 CFR 1000.350; 25 CFR 1000.355; 25 CFR 1000.365.

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: OST is migrating to the TFAS, Innovest Systems LLC, accounting system.

E. Is this information system registered in CSAM?

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

010-000000934, SSP will be entered when the system goes operational.

☐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, 80 FR 1043 (January 8, 2015), which may be viewed at: https://www.doi.gov/privacy/os-notices.

☐No

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

☒ Yes: *Describe*

The Office of Management and Budget (OMB) control number is #1035-004, Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address. Expiration date, 01/31/2020.

☐No

Section 2. Summary of System Data

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

☒ Name

☒ Social Security Number (SSN)
☒ Citizenship
☒ Personal Cell Telephone Number
☒ Gender
☒ Tribal or Other ID Number
☒ Birth Date
☒ Financial Information
☒ Personal Email Address
☒ Group Affiliation
☒ Medical Information
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Other Names Used
☒ Truncated SSN
☒ Mailing/Home Address
☒ Place of Birth
☒ Driver's License
☒ Race/Ethnicity
☒ Other: Beneficiaries' Financial Institution routing and account numbers. Date of death if applicable, Tribal affiliation, blood quantum, taxpayer identification number, contact information for individuals who may know the whereabouts of beneficiaries whose location is unknown.

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:
Information may also be derived from the Social Security Administration, private entities that may provide address information for beneficiaries whose whereabouts are currently unknown, and address information from the U.S. Postal Service.

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
The TAAMS is the system of records for Indian trust real property interests. Information contained in the TAAMS is continually shared with TFAS.

☐Other

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

OST performs trust responsibilities on behalf of the Secretary of the Interior. Certain data elements, including personally identifiable information (PII), are a necessary part of doing business and are not used for other than required or authorized purposes. Trust account holders are required to provide PII in order to obtain the benefit of having an IIM account, OMB #1035-0004, Trust Funds for Tribal and Individual Indians, 25 Part 115, Expiration January 31, 2020. The intended use of PII is to manage the receipt, investment, distribution, and disbursement of IIM account and Tribal trust fund income; provide trust services and information for Indian trust funds program management; manage beneficiary contact including inquiries and requests regarding their trust assets; provide IIM account status to IIM account holders; locate IIM account holders whose whereabouts are currently unknown; document trust account transaction history and quarterly statements; and transfer electronic data to the Department of the Treasury for the processing of IIM account and Tribal trust fund account payments. The use of PII also supports DOI land consolidation activities and provides an interface to TAAMS, DOI's system of records for title and land resource management of Indian trust land within DOI and BIA.

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

☒ Within the Bureau/Office
Any authorized OST employee acting in his or her official capacity. The data allows TFAS to perform essential functions for trust account holders.

☒ Other Bureaus/Offices
Data is shared with BIA real property management systems. The TFAS allows coordination, collaboration and information sharing of beneficiary contact information between OST and BIA. The data allows OST to perform essential functions for trust account holders.

☒ Other Federal Agencies
Data may be shared with the Department of Justice, a court or an adjudicative or other administrative body, or a party in litigation before a court or an adjudicative body, or any DOI employee acting in his or her official capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee, when one is a party to a proceeding

or has an interest in a proceeding; U.S. Postal Service, Internal Revenue Service, and the Social Security Administration, as necessary and authorized to perform essential functions for trust account holders or meet legal and fiduciary obligations. Data may also be shared with the Department of Treasury to disburse trust funds and to issue disbursements, Explanation of Payment reports (EOPs), Statements of Performance (including Assets), IRS Form 1099's, Osage Headright Owners Share of Income, Deductions, etc. Data may also be shared with other organizations as an authorized routine use as outlined in OS-02, IIM Trust Funds, 80 FR 1043, January 8, 2015, which may be viewed at: https://www.doi.gov/privacy/os-notices.

☒ Tribal, State or Local Agencies
Tribes that have contracted or compacted the IIM trust funds program, state and local governments and Tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled, and as authorized as a routine use in OS-02, Individual Indian Money (IIM) Trust Funds, 80 FR 1043, January 8, 2015, which may be viewed at: https://www.doi.gov/privacy/os-notices.

☒ Contractor
Contractors have access to TFAS in order to perform services requiring access to these records on DOI's behalf to carry out the purpose of the system.

☒ Other Third Party Sources
Data may be shared with beneficiaries or to individuals or entities for information of owners of any interest in trust or restricted lands, location of the parcel, and the percentage of undivided interest owner by each individual; other owners of interests in trust or restricted lands within the same Indian Reservation; and others as described in the routine uses section in OS-02, Individual Indian Money (IIM) Trust Funds, 80 FR 1043, January 8, 2015, which may be viewed at: https://www.doi.gov/privacy/os-notices.

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

☒ Yes

Trust account holders provide PII in order to obtain the benefit of having an IIM account, OMB #1035-0004, Trust Funds for Tribal and Individual Indians, 25 Part 115, Expiration January 31, 2020. Respondents voluntarily provide information in order to gain or retain a benefit, such as access to funds held in trust. The intended use of PII is to manage the receipt, investment, distribution, and disbursement of IIM account and Tribal trust fund income; provide trust services and information for Indian trust funds program management; manage beneficiary contact including inquiries and requests regarding their trust assets; provide IIM account status to IIM account holders; locate IIM account holders whose whereabouts are currently unknown; document trust account transaction history and quarterly statements; and transfer electronic data

to the Department of the Treasury for the processing of IIM account and Tribal trust fund account payments. The use of PII also supports DOI land consolidation activities and provides an interface to TAAMS, a system of records for title and land resource management of Indian trust land within DOI and BIA.

☐No

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

☒ Privacy Act Statement

A Privacy Act Statement is provided to individuals on the OST Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address form or over the telephone when they call the Trust Beneficiary Call Center (TBCC).

☒ Privacy Notice

Notice is also provided to individuals through the publication of this privacy impact assessment and the OS-02, Individual Indian Money (IIM) Trust Funds, system of records notice, 80 FR 1043 (January 8, 2015), which may be viewed at: https://www.doi.gov/privacy/os-notices.

☒ Other: *Describe each applicable format.*

The DOI security banner alerts all authorized users of the system and DOI network that they are subject to monitoring and have no expectation of privacy.

☐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 by identifiers linked to trust account holder such as name, SSN, IIM or Tribal trust fund account number(s), Tribal affiliation, Tribal enrollment or census number(s), Tribal codes, electronic ticket numbers, contact names, call numbers or incident number(s), appraisals, parcels or encumbrances on ownership, or by organizational links such as Tribal trust fund account codes.

I. Will reports be produced on individuals?

☒ Yes

Reports generated internally that are used for tracking work and managing accounts may be used by Field Operations, Trust Services, and the Office of Trust Review and Audit, and authorized staff within OST.

☐No

Section 3. Attributes of System Data

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

Data collected directly from individuals is presumed to be accurate at the time of submission and individuals have the opportunity to update their information at any time to ensure it remains accurate. The data is verified for accuracy by the submitting entity and through updates or amendments, as needed, by authorized OST users. Authorized users are responsible for verifying data based on their access level and job duties.

B. How will data be checked for completeness?

Data collected directly from individuals must be complete at the time of submission and individuals have the opportunity to update their information at any time to ensure it is complete. Manual pre- and post-quality assurance (QA) processes are in place, daily reconciliation with Treasury occurs, and data is checked for completeness by the submitting entity and the system itself. It is also the responsibility of the authorized users entering the data into the system to check for completeness of the data. Authorized users are responsible for ensuring the information is correct by verifying the information.

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

Individuals have the opportunity to update their information at any time to ensure it remains current. Steps to ensure data is current are located in the Trust Services Desk Operation Procedures manual. Data is entered and updated on a regular basis.

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

The National Archives and Records Administration (NARA) approved retention schedule for OST is the Indian Affairs Records Schedule (IARS). The TFAS system is scheduled in the IARS as TR-6171-P and approved as permanent data (NARA Job #N1-075-04-7). TFAS data will be migrated into the new electronic information system supported by Innovest and maintained within the system until disposition is required. The business functions and data

capture requirements are the same from the TFAS system to be migrated to a new application. The data retention will not change with the migration.

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

Data and information maintained within TFAS are retained under the appropriate NARA approved Records Schedules (IARS). Data disposition follow the NARA guidelines and approved Records Schedule for transfer, pre-accession and accession activities to NARA. These activities will also comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and OST Records Management policies and procedures.

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 individual privacy due to the type and volume of sensitive PII maintained in the system related to the individual's name, address, phone number, date of birth, date of death, SSN, Tribal affiliation, financial documents, account number(s), and other categories of records associated with financial and investment activity. This risk is mitigated through management, operational, and technical controls that are implemented to protect the confidentiality, integrity, and availability of the information.

There is a risk that individuals may not have notice of the purpose for collecting their information or how it will be used. Individuals are notified of the purpose of collecting information, its intended uses, and OST privacy practices through the Privacy Act statement provided on OST's Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address form, the published OS-02, Individual Indian Money (IIM) Trust Funds, system of records notice, 80 FR 1043 (January 8, 2015), and this privacy impact assessment, which provides a detailed description of the data elements and how the data will be used and shared.

There is a risk that more information may be collected than is necessary. This risk is mitigated by only using the minimal amount of information necessary to effectively meet the requirements for conducting trust funds accounting and investments. There is a risk of maintaining inaccurate information in TFAS that may result in incorrect determinations. This risk is mitigated through established quality control procedures to check the completeness and accuracy of information before entering data into TFAS. In addition, access is restricted to only authorized users that are allowed to enter data into the system with a "need-to-know" to perform their official duties.

There is a risk that unauthorized individuals could potentially gain access to the PII on the system. This risk is mitigated by implementing security and privacy controls to protect the data, including technical controls to restrict and manage access and granting access to authorized personnel based on the least privilege principle to perform official duties. The vendor (contractor) Innovest is undergoing the Authorization and Accreditation (A&A) for the application, Software as a service (SaaS) and the FedRAMP certification process for the SaaS. The accreditation boundary for the Innovest Trust & Wealth Management Solutions service includes applications and components that reside on Amazon Web Services (AWS) Infrastructure-as-a-Service (IaaS) in the AWS GovCloud region. The Trust & Wealth Management Solutions service inherits IaaS security controls from the AWS FedRAMP package for AWS GovCloud, which are documented in the AWS GovCloud FedRAMP System Security Plan. Electronic records are maintained in accordance with the OMB, DOI and FedRAMP guidance reflecting the implementation of the Federal Information Security Modernization Act (FISMA) of 2014 and the Privacy Act. Electronic data is protected through user identification, passwords, database permissions and software controls, and different access levels are established for different types of users. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training, including role-based security and/or role-based privacy training and sign the OST Rules of Behavior before authorized to access the system. The use of OST/DOI IT systems is conducted in accordance with the appropriate OST/DOI use policy. All access is controlled by authentication methods to validate the authorized user.

There is a risk that some data may not be appropriate to transfer or that the contractors may not handle information according to DOI policy. Innovest is a cloud system rated as a FISMA Moderate system and requires management, operational, and technical controls in accordance with the NIST SP 800-53 as mandated under the FedRAMP certification process to mitigate privacy risks for the unauthorized access, disclosure, or misuse of PII. Access is limited to authorized users during the collection, use, retention, processing, disclosure, and potential destruction of information. A security plan was completed to address security controls and safeguards for the Innovest Cloud system. Controls are outlined in the Innovest Cloud System Security Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, and includes the use of role-based training, encryption, and maintaining data in secure facilities, among others. Innovest protects information that is “at rest” for confidentiality and integrity purposes. Backups are stored encrypted within SQL server file system. Innovest uses AES 256-bit encryption for both the Elastic Block Store (Amazon EBS) volumes and the Amazon Simple Storage Service (Amazon S3) components to store information cryptographically at rest. Innovest has cryptographic

mechanisms implemented to prevent unauthorized disclosure and modification of all customer data collected by Trust & Wealth Management Solutions.

An audit trail of activity will be maintained sufficient to reconstruct security relevant events. The audit trail includes the identity of user's 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 are reported to OST IT Security. The OST 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 must 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.

Innovest Systems, Trust & Wealth Management Solutions (TFAS) implements audit logging mechanisms for the information systems and its applications. Splunk is utilized for near real-time audit logging and reporting as the centralized SIEM solution for security monitoring, advanced threat detection, insider threat analysis, incident investigation and forensics, incident response planning, compliance management, and fraud detection. Innovest's audit logging is utilized to assess Innovest's security posture in the identification of potential incidents or compromised systems by monitoring for vulnerabilities that lead to breaches. The Splunk solution is utilized for account monitoring by maintaining a consistent and accurate monitoring process of account and data access. In addition, Splunk monitors and logs for compliance purposes by establishing a historical baseline and understanding the scope and data in Innovest's infrastructure and comparing log information for anomalies. Web application auditing and logging takes place within the application to establish an audit trail of events taking place within the Innovest application. Splunk is further utilized to automatically pull the logging information from the audit logs created by the application into the Splunk centralized solution for analysis.

Innovest has conducted risk assessments against their information systems and their environment. It included the likelihood and magnitude of harm resulting from unauthorized events such as unauthorized access, use, disclosure, disruption, modification and destruction of data. The risk assessment results are documented in a formal security assessment report (SAR). OST and applicable Innovest Trust & Wealth Management Solutions personnel reviewed documented risk assessment results.

There is a risk that information in TFAS may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored in limited to the minimal amount of data needed to meet OST's mission and business functions. Records are maintained in accordance with records retention schedules that are approved by NARA. Users are also reminded through policy and training that they must follow the applicable retentions schedules and requirements of the Federal Records Act. The data in TFAS are closely safeguarded in accordance with applicable laws, rules, and policies.

There is a risk that PII may be exposed by authorized users. This risk is mitigated by ensuring that proper safeguards are in place in accordance with 43 CFR 2.226. 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. 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 annual Federal Information Systems Security Awareness, Privacy and Records Management training courses. Contract employees are monitored by their Contracting Officer Representative (COR) and the Associate Chief Information Security Officer (ACISO).

There is a risk in the process of migrating trust data to the new vendor Innovest. This risk is mitigated by using a Secure File Transfer Protocol (SFTP), which ensures that data is securely transferred using a private and safe data stream. SFTP requires that the client user must be authenticated by the server and the data transfer must take place over a Secure Shell (SSH) which is a cryptographic network protocol.

OST employees must take privacy, Federal Information Systems Security Awareness (FISSA), and records management training prior to being granted access to OST information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure and understanding of the responsibility to protect privacy. OST personnel also sign the OST 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

The data allows OST to perform essential functions for trust beneficiaries and Tribes.

☐No

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

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

☒ No

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

☐Yes: *Explanation*

☒ No

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

☐Yes: *Explanation*

☒ No

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

Not Applicable. The system does not derive new data.

F. Are the data or the processes being consolidated?

☐Yes, data is being consolidated.

☐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

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

All authorized OST users have access to view account information. Specific staff have authority to process cash, asset, account, and name/address information based on their job function. Access to TFAS 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 authorized access to the system are monitored by the COR and ACISO.

The Information System Owner, system manager, and supervisors determine 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.

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.

For TFAS routine file maintenance audit records are maintained that identify when account asset, name/address information is created, maintained/changed and deleted. TFAS system logs capture date and time users log in and any changes that are initiated.

☐No

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

TFAS does not monitor members of the public. 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 user's may include username, failed attempts, files accessed, and user actions. In this type of actionable reporting any and all of the users actions can be reported. TFAS system logs capture date and time users log in and any changes that are initiated. 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 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 COR and ACISO.

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

Access to TFAS 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. An audit trail of activity will be maintained sufficient to reconstruct security relevant events. Audit logging is utilized to assess security posture in the identification of potential incidents or compromised systems. The system performs account monitoring by maintaining a consistent and accurate monitoring process of account and data 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 COR 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 Associate Chief Information Officer (ACIO) is the Information System Owner (ISO) and the official responsible for oversight and management of the TFAS (Innovest) security controls and the protection of any information processed and stored in the TFAS. The Information System Owner and the Information System Security Officer (ISSO) 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 TFAS. These officials and authorized TFAS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for working with the Privacy Act system manager to meet the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with OST Associate Privacy Officer (APO).

The vendor and cloud service providers are also responsible for the protection of PII, incident reporting, and other privacy controls to ensure adequate safeguards are implemented in accordance with the appropriate Federal laws, regulations, and Departmental policies.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ISO is responsible for oversight and management of the system security, and privacy controls. The ISO and ISSO are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.