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: OSTNet, OST Local Area Network (LAN)/Wide Area Network (WAN) (OST LAN/WAN)
Bureau/Office: Office of the Special Trustee for American Indians (OST)
Date: September 30, 2020
Point of Contact:
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: privacy_ost@ost.doi.gov
Phone: (505) 816-1645
Address: 4400 Masthead St. NE, Albuquerque, NM 87109

Section 1. General System Information

A. Is a full PIA required?

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

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Office of the Special Trustee for American Indians (OST) OSTNet (Local Area and Wide Area Networks (LAN/WAN)) is a General Support System (GSS) which consists of both local and wide area network components. The OST GSS houses minor applications (subsystems) which operate from the GSS as a set of Information Technology (IT) resources that are within and across OST Offices that provide mission support operations.

OSTNet, the GSS consists of infrastructure and an administrative network that consists of servers, workstations, networking devices (routers, firewalls, and switches), storage devices, backup devices, and print devices. Services provided by GSS include encryption protection, virus/malware protection, Voice over IP (VoIP), system management, backup, vulnerability scanning, and Active Directory (AD).

OSTNet, the GSS includes SharePoint, which provides a Web page user interface, enterprise collaboration, and project management services. SharePoint users may post information, documents, spreadsheets, PDFs, graphics, etc. to share or collaborate via a secure encrypted internal website. DOI hosted SharePoint content sites are owned and administered by OST personnel from various subscribing DOI bureaus and offices.

OST's trust responsibilities on behalf of the Secretary of the Interior are to manage the receipt, investment, distribution, and disbursement of individual Indian Money (IIM) account and Tribal trust fund income; compliance with the American Indian Trust Fund Management Reform Act of 1994; and, to improve accountability and management of Indian funds held in trust by the Government.

This PIA covers the OSTNet. Hosted applications and sub-systems are covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses personally identifiable information (PII).

C. What is the legal authority?

American Indian Trust Fund Management Reform Act of 1994 (P.L. 103-412), 108 Stat. 4239; 25 USC 4001, 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); Public Law 93-638 Self-Governance Compacts; 25 USC 4041, 25 USC §5363 (d) (1), 25 CFR 1000.350, 25 CFR 1000.355, 25 CFR 1000.365; OMB Directive M-12-18, *Managing Government Records*; OMB Circular A-130, *Managing Information as a Strategic Resource*; Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*; Presidential Memorandum, *Managing Government Records*.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection

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

E. Is this information system registered in CSAM?

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

010-000000900 010-000000901 010-000000902 010-000000906 010-000000910 010-000000911 010-000000913 010-000000914, 010-000000915 010-000000916 010-000000917 010-000000918 010-000000919 010-000000920 010-000000923 010-000000924 010-000000927 010-000000928 010-000000932, 010-000001858; OST LAN/WAN SSP. (OST LAN_WAN UII Codes 2018.doc, are located under miscellaneous documents)

☐ 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.*
	See addendum		

Due to the nature of the OSTNet in providing hosting services to OST for mission support operations, there are numerous minor applications or subsystems that are hosted in OSTNet. Hosted applications and systems are identified in the OSTNet record in CSAM, and are covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses PII.

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)*

OSTNet is associated with multiple applications that are housed on the GSS. Records associated with hosted applications may be covered by Government-wide or DOI Privacy Act system of records which may be viewed at http://www.doi.gov/privacy/sorn.

SORNs related to OSTNet and mission areas include:

IIM Trust Funds – Interior, OS-02, 84 FR 44321, August 23, 2019 covers individual Individual Indian money trust funds rerecords.

DOI-46, Physical Security Access Files - January 21, 2020, 85 FR 3406.

DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - March 12, 2007, 72 FR 11040.

DOI-85, Payroll, Attendance, Retirement, and Leave Records - July 19, 2018, 83 FR 34156.

Financial records are covered under DOI-86, Acquisitions of Accounts Receivable: FBMS - July 28, 2008, 73 FR 43772; DOI-87, Grants and Cooperative Agreements: FBMS - July 28, 2008, 73 FR 43776; DOI-88, Travel Management - July 28, 2008, 73 FR 43769; and DOI-89, Grants and Cooperative Agreements: FBMS - July 28, 2008, 73 FR 43775.

OPM/GOVT-1 General Personnel Records, which may be viewed at: https://www.opm.gov/information-management/privacy-policy/#url=SORNs

GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS), October 23, 2015, 80 FR 64416 which may be viewed at: https://www.gsa.gov/reference/gsa-privacy-program/systems-of-records-privacy-act/system-of-records-notices-sorns-privacy-act

☐ No:

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

☒ Yes: *Describe*

OSTNet hosted systems have two OMB Control Numbers:

Individual Indian Money (IIM) Instructions for Disbursement of Funds and Change of Address, OMB Control No. 1035-0004, expires 10/31/2020.

Trust Evaluation System, OMB Control No. 1035-0005, expires 12/41/2020.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Security Clearance
☒ Personal Cell Telephone Number
☒ Spouse Information
☒ Tribal or Other ID Number
☒ Birth Date
☒ Financial Information
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Other Names Used
☒ Employment Information
☒ Truncated SSN
☒ Education Information
☒ Military Status/Service
☒ Emergency Contact
☒ Mailing/Home Address
☒ Place of Birth
☒ Driver's License
☒ Race/Ethnicity
☒ Other: *Specify the PII collected.*

PIV credentials are required for access to the OSTNet, GSS. User Name and Password credentials are allowed when PIV card is unusable. DOI Active Directory (user object) contains user name, display name, and are populated by the US/DOI Access system. Hosted applications may include various types of PII selected or other information about individuals that are contained in DOI records. This PIA covers the OSTNet. Hosted applications and sub-systems are covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses PII. See addendum and related PIAs for PII in the specific systems.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☒ Other: *Describe*

No PII is collected by OSTNet, GSS. PIV credentials are required for access to the GSS. User Name/Password credentials are allowed when PIV card is unusable. DOI Access is the source for username and password. This PIA covers the OSTNet. Hosted applications and sub-systems are covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses PII. See addendum and related PIAs for PII in the specific systems.

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 - Hosted applications that contain PII use existing data from DOI Access, DOI records, Bureau of Indian Affairs (BIA), Office of Natural Resource and Revenue (ONRR), and Treasury systems; Accounting Reconciliation Tool (ART), Trust Funds Accounting System (TFAS). Users of OSTNet utilize information taken (shared) from other sources to create work products (reports, analytical spread sheets, etc.) via office automation tool such as MS Office. OSTNet serves as a conduit, transfer point for interface files to share information. AD user data is provided by interface with DOI Access and is also provided by individual users during the account creation or updating process. See addendum and related PIAs for PII in the specific systems.

☒ Other: *Describe*

Hosted applications are identified in the OSTNet record in CSAM, and are covered by separate PIAs that will indicate how the PII is collected. See addendum and related PIAs for PII in the specific systems.

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

OSTNet is a GSS designed to host a variety of systems. The GSS does not collect or process PII for hosted systems. OSTNet serves as a conduit, transfer point for interface files to share information. Use of PII are to support OST's mission. OSTNet provides hosting services to OST for mission support operations. Hosted applications are identified in the OSTNet record in CSAM, and are covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses PII. See addendum and related PIAs for intended uses of PII of the specific systems.

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.*

The OSTNet, GSS does not share PII for hosted systems. Hosted applications that contain PII use existing data from DOI Access, DOI records, OST, Information may be shared between the OST ART, TFAS, and related OST applications by authorized users to perform official duties. Users of OSTNet utilize information taken (shared) from other sources to create work products (reports, analytical spread sheets, etc.) via office automation tool such as MS Office. OSTNet serves as a conduit, transfer point for interface files to share information. Hosted applications have PIAs and will identify other programs within OST with whom information is shared. See addendum and related PIAs for specific sharing of PII within OST.

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

The OSTNet, GSS does not collect or process PII for hosted systems. Hosted systems may share information with BIA, Bureaus of Indian Education (BIE), Bureau of Safety and Environmental Enforcement (BSEE), ONRR, Office of the Secretary (OS) and Interior Business Center (IBC), Office Valuation Services (OVS), Office of Hearing and Appeals (OHA), and other bureaus and office. Data shared supports OST's mission. Hosted applications have PIAs and identify other bureaus/offices with whom information is shared. See addendum and related PIAs for specific sharing with other bureaus and offices.

All access to the OSTNet, hosted applications and actions by authorized users can be reviewed for auditing purposes or security monitoring and management of user accounts. Information on security incidents may be shared with DOI officials and oversight organizations as required by Federal policy.

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

The OSTNet, GSS, does not collect or process PII for hosted applications. Hosted applications may be shared outside DOI with the Department of Justice (DOJ), Department of Treasury Internal Revenue Service (IRS), Office of Management and Budget (OMB), Office of Inspector General (OIG) to perform annual, financial, reviews or audits, and Social Security Administration (SSA), U.S. Postal Service (USPS), and the

Government Accountability Office (GAO) to perform annual, financial, reviews or audits. Hosted applications have separate PIAs and identify other Federal Agencies that information may be shared with. See addendum and related PIAs and SORNs for external sharing with other Federal agencies, which may be viewed on the DOI PIA and SORN websites.

All access to the OSTNet, hosted applications and actions by authorized users can be reviewed for auditing purposes or security monitoring and management of user accounts. Information on security incidents may be shared with DOI officials and oversight organizations as required by Federal policy.

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

PII associated with hosted applications may be shared with Tribal organizations that contract OST programs or services to carry out OST's mission. Data may be shared is provided for the performance of official functions. Information may be shared with Tribes who perform services or otherwise support OST or DOI activities. Hosted applications have separate PIAs and identify other entities outside DOI that information may be shared with. See addendum and related PIAs for specific sharing with other Tribal, state, or local agencies.

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

The OSTNet, GSS, does not collect or process PII for hosted applications. PII associated with hosted application may be shared with contractors (including employees of the contractor) of OST to perform services and require access to the data on OST's behalf to carry out the purposes of the mission. Hosted applications have separate PIAs and identify other entities outside DOI that information may be shared with.

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

PII associated with hosted applications are shared with authorized external third party entities in support of OST's mission or functions. OSTNet serves as a conduit, transfer point for interface files to share information. Hosted applications have separate PIAs and identify other entities outside DOI that information may be shared with. See addendum and related PIAs for specific sharing with other third-party sources.

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.*

Information is voluntarily provided by employees in order to obtain access to the DOI network and information systems. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment at DOI they will not be given access to the network and may be unable to perform their duties. PII for the OSTNet, GSS, is originally collected by DOI Access

via the consent and notice process. Hosted applications will indicate if individuals have opportunity to decline to provide information or to consent to specific uses of their PII, accordingly. See addendum and related PIAs.

☐ No

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.*

OSTNet is a GSS that hosts numerous information systems. Data on users is provided by DOI Access created through a form containing a Privacy Act Statement (PAS); Information provided to an individual when asked to provide PII data is described in the appropriate PIA and SORN associated with the particular information system. The relevant PAS properly identify the authority for the collection of information, purpose of the collection, routine use of the PII and disclosure of information, that consists of furnishing of the information is voluntary; however, the failure to furnish the requested information will prevent the user from accessing or authenticating to the DOI network. Hosted applications have separate PIAs that will cover what information is provided to an individual when asked to provide PII data.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through this PIA. OSTNet is a GSS that hosts numerous systems. Hosted information systems (applications) have PIAs and SORNs that indicate what information is provide to individuals when asked to provide PII, as applicable. All users are provided with a Privacy Notice that warns of the privacy requirements, consent to monitoring, and references the DOI Privacy Act regulations and applicable Privacy Act penalties when accessing the DOI network

☒ Other: *Describe each applicable format.*

At logon to the network users and system administrators receive the DOI security banner alerts all authorized users (holders of both regular and administer accounts) of the system and DOI network that they are accessing a DOI system, are subject to monitoring and there is no expectation of privacy during use of the system. Hosted applications have PIAs and SORNs that indicate what information is provide to individuals when asked to provide PII, as applicable.

☐ 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 associated the active directory can be retrieved by name, username, workstation name, and active directory group. Retrieval occurs when resetting passwords, to change permissions, transfer or move accounts, and add/remove workstations. Applications that reside on the GSS may be retrieved by name, SSN or truncated SSN, address, Tax Identification Number (TIN), account number, Tribe name, Tribal enrollment or census number, electronic ticket number, case number, email, phone or cell numbers, and other identifiers linked to individuals. Hosted applications have separate PIAs and will indicate how relevant data is retrieved. See addendum and related PIAs.

I. Will reports be produced on individuals?

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

OSTNet does not produce reports on individuals. Audit logs track user activity in accordance with DOI logging requirements. The logged information is used for investigative actions associated with cyber security incidents. The OSTNet is a GSS designed to host a variety of applications. All applications that reside on the GSS have a separate PIA which assess and address the relevant privacy risks specific to the applications and will indicate if reports are produced on individuals. See addendum and related PIAs .

☐ No:

Section 3. Attributes of System Data

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

OSTNet data is obtained from other DOI systems and records. The accuracy of data is critical for OST and DOI, and must be maintained to ensure protection of individual privacy; applications hosted by the OSTNet are under the control and ownership of each system owner, system manager, and OST program officials. Applications that reside on the GSS have PIAs that address how data from other sources are verified for accuracy.

B. How will data be checked for completeness?

OSTNet data is obtained from other DOI systems and records. Due to the nature of the OSTNet as a GSS, there are numerous applications and systems hosted in the OSTNet that may collect, maintain or process PII. Applications that are housed on the GSS have separate PIAs that identify and describe how data is checked for completeness.

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

Certain updates may take effect via the AD system updates, however; it is up to the individual to update their contact information and update data in any application and/or system that is hosted within EHI. DOI provides the My Account (https://myaccount.doi.gov) site where users can maintain and update their work related contact information. Users are notified that it is their responsibility to ensure their information is up to date. As a function of AD, all data related to user access is continuously synchronized across the entire system. Hosted applications have separate PIAs to assess privacy risks and system owners are responsible for ensuring current information.

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

Records and data maintained in OSTNet, GSS are retained in accordance with the Departmental Records Schedule (DRS) – Administrative schedule 1.4.1 – [0013] Short Term IT Records – System Maintenance and Use, approved by the National Archives and Records Administration (NARA). The records encompass IT files that are not needed for extended retention. Records are characterized by being necessary for day-to-day operations. Other applications' retention period varies. Generally, these are maintained for the duration of the requirement for the account, but 60-90 days after non-use, termination, cancellation the account would be removed. For general system records, the retention schedules are DRS 1.4.A(1) DAA-0048-2013-0001-0013, DRS 1.4.A(2) DAA-0048-2013-0001-0014, and DRS 1.4.B DAA-0048-2013-0001-0015. The dispositions are temporary, the cutoff vary depending on the types of files, and the records will be destroyed no later than 3 years after cutoff for records covered under record schedule DRS 1.4.A(1) DAA-0048-2013-0001-0013 and DRS 1.4.A(2) DAA-0048-2013-0001-0014, or no later than 7 years after cutoff for the records covered under record schedule DRS 1.4.B DAA-0048-2013-0001-0015. System backups vary in duration of retention requirement, but generally 90 days of backups have potential for restoration that would contain user account data that could be tied to full name. The request forms (add/changes or deletes) for privileged accounts are maintained indefinitely, and therefore the correlation to past accounts could be verified if needed.

Records and data maintained in OSTNet, applications that are housed on the GSS, are the responsibility of the information system owner, system manager, and OST program officials. Retention periods will vary, depending on the information system, program functions, and subject matter of the records and data. Hosted applications have separate PIAs with records retention for data in the associated information system.

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

Data associated that are associated with OSTNet, applications that reside on the GSS are disposed or remove in accordance with applicable retention schedules. Procedures for disposition of the data stored in individual applications will vary by application. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate DRS approved by NARA, OST and DOI records policy, and 384 Departmental Manual 1.

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 moderate risk to individuals associated with OSTNet and the hosted applications that reside on the GSS due to the volume of sensitive PII maintained. PII includes name, username, work email address, work phone number, and other work related contact information. This risk is mitigated through administrative, physical, and technical controls that have been implemented to protect the confidentiality, integrity, and availability of the information.

There is a risk that PII may be misused or used for unauthorized purposes. DOI authorized personnel sign the DOI Rules of Behavior (ROB) and are subject to monitoring in the system and DOI network. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties. DOI employees must take privacy, FISSA, and records management training prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based Privacy Awareness training initially and annually, to ensure an understanding of the responsibility to protect privacy.

OSTNet, GSS, has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST). The OSTNet is rated as a FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII and other sensitive information contained in the system.

There is a risk of unauthorized access. The OSTNet has developed a System Security and Privacy Plan based on NIST guidance and is part of a Continuous Monitoring Program (CMP) that includes ongoing security and privacy control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. As part of the CMP continual auditing occurs on the GSS to identify and respond to potential impacts to PII information stored within the environment, which will help the agency effectively maintain a good privacy and security posture for the system. Security and privacy awareness training is required for all OST/DOI employees and information system users

(including manager and senior executives) before authorizing access to information systems, and sign the OST/DOI Rules of Behavior. Security and Privacy role-based training is also required for those with special roles and privileges.

There is a risk that the individual may not know or consent to the uses of their information once it is collected. This risk is mitigated through the Privacy Act Statements provided to individuals, Privacy Act Statements provided through various OST and DOI during the performance of official duties, and publication of this privacy impact assessment, and applicable system of record notices that cover PII associated with the applications that reside on the GSS.

There is a risk that information in the OST and DOI information system or applications will be maintained longer than necessary to achieve the OST and DOI mission, or that records may not be properly destroyed. This risk is mitigated by managing records in accordance with a NARA-approved records schedule and providing extensive training to users on IT security, Privacy, Records Management and controlled unclassified information. This training specifically includes handling and disposal of records with sensitive information and also the proper procedures for handling faxed information.

There is a risk that PII may not be accurate. OSTNet and applications that reside on the GSS are associated with Active Directory and DOI Access which has data validation checks in place to identify any discrepancies such as incomplete or duplicated data.

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*

OSTNet, GSS hosted applications, data is required or are necessary for the purpose for which the systems are developed. The GSS is associated with DOI Access. The PII data in the DOI Active directory is necessary for identity management and required under Federal mandates.

☐ 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 OSTNet, GSS, does not create new data, and therefore will not be verified for relevance and accuracy. The applications that reside on the GSS have separate PIA that identify how data is verified for relevance or accuracy. Data may be verified for relevance and accuracy by authorized users associated with hosted applications.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

Users and contractors will have access to their own information, and in some cases a limited subset of other users based on mission, system, and application management needs. Contractors working for OST and DOI fall into the same category as "All Users".

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

OSTNet, hosted application, access to data is restricted through established permissions and access controls. System administrators have access based on need to know and mission accomplishment. User access is also controlled by system profile and based on roles, responsibilities and access requests from data owners. Access to data is restricted to authorized users and personnel who have a need to know to perform their duties. Access is further governed by DOI and OST IT security policy and protection of personal information. Data that resides on the GSS (in hosted systems/minor applications) are safeguarded in accordance with applicable security rules and policies.

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?*

OSTNet does not involve contractors. Hosted applications that reside on the GSS may involve contractors with design, development, or maintenance, and the appropriate contract clauses were included in each contract.

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*

OSTNet hosted systems data input and changes can be tracked. All user activity is audited as part of the security monitoring and management of user accounts and can be reviewed by Security personnel; all user actions taken on OST/DOI IT systems are audited; the information includes items such as: failed login/access attempts, changes in user permissions, etc., that are associated with user authentication. For routine file maintenance audit records are maintained that identify when account asset, name/address information is created, maintained/changed and deleted. System logs capture date and time users log in and any changes that are initiated.

As part of the security monitoring and management of the system all user actions taken on OST and DOI resources are audited and can be reviewed by designated administrators. This information includes items such as: username, login date/time/location, failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

☐ No

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

All access to the OSTNet, hosted applications, and actions by authorized users can be reviewed for auditing purposes. Audit reports are customizable and may include, but are not limited to, unique applicant ID logon/logoff timestamps; data accessed and or/modified; and permission changes. 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.

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

Access to administrative functions such as audit logs and monitoring is strictly controlled. Only administrators and personnel with an official "need to know" can perform these functions. DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail includes the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

All authorized users must complete annual FISSA training, Privacy Awareness, Records Management training, and sign the OST/DOI Rules of Behavior before granted access to any DOI and OST IT resources, and annually thereafter. System administrators and security personnel with access to DOI and OST records have additional role based training requirements.

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 IT Director serves as the OSTNet Information System Owner (ISO) and the official responsible for oversight and management of the OSTNet security and privacy controls and the protection of OST data processed and stored within associated hosted

applications that reside on the GSS. The ISO, Associate Chief Information Security Officer (ACISO), and authorized system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the hosted applications, and addressing Privacy Act requests for notification, access, amendment, and complaints in consultation with OST and 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 IT Director, as the OSTNet ISO is responsible for the daily operational oversight and management of the OSTNet security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The OSTNet ISO, ACISO, 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, within 1-hour of discovery in accordance with Federal policy and established OST/DOI procedures, and for working with the APO and Departmental Privacy Officer to ensure appropriate remedial activities are taken to mitigate any impact to individuals.

Addendum

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.*
Automated Clearing House Broadcast Notification - Attention Software (ACHBN)	Notify beneficiaries on deposits to their checking/savings accounts from the Trust Funds Accounting System (TFAS) via web, text, email, or voice mail notification.	No	This application supports OST mission-related business functions.
Automated Clearing House (ACH) RFM	Allow the beneficiary to determine if they want notification by email, text message, or no message.	Yes	Name, financial information. Privacy Act records are covered by the OS-02, Individual Indian Money (IIM) Trust Funds System of Records Notice (SORN).
Auto-Audit (AA)	Audit planning, scheduling, monitoring, and creating audits; to perform risk assessments, compile data related to audit coverage and strategic planning, reporting, issue tracking; expense & time reporting and quality assurance.	Yes	Name, Social Security Number (SSN), cell/phone number, gender, spouse information, Tribal or other identification (ID) number, birth date, financial information, email address, group affiliation, medical information, mother's maiden name, marital status, disability information, child or dependent information, other names used, employment information, truncated SSN, emergency contact, mailing address, place of birth, driver's license, race/ethnicity, date of death, Tribal affiliation, blood quantum, taxpayer identification number (TIN). Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Auto One-Time Disbursements/Daily	One time disbursements of funds to beneficiaries.	No	This application supports OST mission-related business functions.
Box Index Search System (BISS)	Create a file and document level listing of the contents of boxes of inactive records retired from OST, Bureau of Indian Affairs (BIA), other trust bureaus, and some tribes after they have met their retention period; tracks Records Move Requests which authorize boxes of records to be moved from the field to the AIRR, SF-135 forms and box inventories that accession boxes into the National Archives and Records Administration	Yes	Name, religious preference, SSN, citizenship, security clearance, cell/phone number, gender, spouse information, Tribal or other ID number, birth date, financial information, email address, group affiliation, medical information,

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
	(NARA) and Research Requests; provides authorized users a tool to search for inactive records at the file or document level for litigation and non-litigation research; allows centrally managed access to inactive records; and allows Indian Affairs staff and contractors direct access to information about inactive records.		mother's maiden name, marital status, disability information, biometrics, credit card number, child or dependent information, other names used, law enforcement, employment information, truncated SSN, education information, military status/service, emergency contact, mailing address, place of birth, driver's license, race/ethnicity. Privacy Act records are covered by OS-3, BISS SORN.
Control Desk - WebBased	Track batches of work done by the Department of Trust Funds Accounting (DTFA).	Yes	Name, beneficiaries' financial information, institution routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Daily Account Distribution System (DADS)	Distribute amounts and interest to IIM accounts.	Yes	Name, SSN, beneficiaries' financial information, institution routing, and account number. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Debit Card Setup Web	Establish IIM accounts for disbursement from debit cards entered and approved by the Field Operations, Trust Beneficiary Call Center (TBCC).	Yes	Name, SSN, beneficiaries' financial information, institution routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
File Copy 1099 - Forms 2007	Allow users to view past copies of 1099s sent to beneficiaries.	Yes	Name, SSN, address, and beneficiaries' financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Indian Trust Systems Query (ITSQ)	Provide a search capability, detailed view of a beneficiary IIM account and access to financial beneficiary information regarding invoices, distributions, property, encumbrance information, etc.	Yes	Name, birth date, SSN, cell/phone number, email address, mother's maiden name, mailing address, and beneficiaries' financial information, routing and account numbers. Privacy

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
			Act records are covered by the OS-02, IIM Trust Funds and BIA-04, TAAMS SORNs.
Liabilities	Pay liabilities for IIM accounts that have a liability and an account balance greater than zero.	Yes	Financial information, beneficiaries' routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Limited Pay	Credit amounts back to IIM accounts for checks greater than fifteen months old.	Yes	Financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Office of Appraisal Services Information System (OASIS)	Record requests for appraisals and review from BIA and the Office of Appraisal Services (OAS).	Yes	Name, mailing address, beneficiaries land ownership, and trust assets. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Office of Natural Resource Revenue (ONRR) Cash Transfer	Take input files (Oil and Gas Royalties) directly uploaded by ONRR personnel and creates transactions in TFAS to match deposits ONRR has made to Treasury, deposit funds into Tribal accounts (determined by tables held in the system), and an IIM holding account.	No	This application supports OST mission-related business functions.
OST DUES	Serve as an enterprise tracking system used by the Principal Deputy Special Trustee (PDST) to assign tasks throughout OST.	Yes	Name, other names used, truncated SSN, place of birth, SSN, Tribal or other ID number, and beneficiaries' financial routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Office of Trust Records (OTR) Database System	Track records management training and technical assistance.	No	This application supports OST mission-related business functions.
Pay.gov (PAYGOV)	Updates lease data that has been processed through pay.gov. and enters the deposit document number for credit cards through the web interface once entered files are created and sent to TAAMS.	No	This application supports OST mission-related business functions.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Per Capita	Distribute per capita amounts to minor and adult non compos mentis IIM accounts, and post the amounts through TFAS.	Yes	Name, address, and beneficiaries' financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Personnel Investigation Tracking System (PITS)	Track OST personnel background investigations and reinvestigations to establish that applicants or incumbents are suitable for the job and/or eligible for a public trust or sensitive position.	Yes	Name, citizenship, gender, birthdate, other names used, place of birth, security clearance, SSN, employment information. Privacy Act records are covered by the DOI-79, Interior Personnel Records.
Returned Checks	Return payment amounts to IIM accounts that have recently had returned checks/ACHs; and update TFAS so the accounts can have the payment amounts distributed back to their IIM accounts.	Yes	Name, beneficiaries' financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Returned Per Capita Account Reconciliation System (RPCARS)	Track funds returned from per capita and serve as a tool for the management of returned per capita tribal accounts by identifying each receipt by individual name, tribal or other ID number.	Yes	Name, financial information, SSN, Tribal or other ID number. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Risk Management Plus (RMP)	Assess program risk conducted by Risk Management.	No	This application supports OST mission-related business functions.
Royalty Account Reconciliation Engine (RARE)	Provide information about funds collected by ONRR and distributed through the holding account.	Yes	Name, address, financial information. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Special Deposit Accounting Prospectus (SDA PRO)	Track aging receipts in Special Deposit Accounts.	No	This application supports OST mission-related business functions.
OST Solicitor Request Tracking System (SOLTRACK)	Track requests that are submitted to the Office of the Solicitor (SOL) from the Principal Deputy Special Trustee (PDST) and Field Operations (FO) for review of legal referrals.	Yes	Name, SSN, beneficiaries' financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Staff Directory	Maintain OST staffing tables, by the Chief of Staff (COS), allow users to look-up OST users work address and phone information; maintain authorized government positions within OST to include vacant positions and contractors; and grant access to build applications on the OST SharePoint site.	Yes	Employee name and photo (optional). Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.
Statement Frequency update/Monthly	Update IIM accounts statement frequency according to data with the access database.	No	This application supports OST mission-related business functions.
TFAS Routine File Maintenance (RFM) Audit Search (TFAS RFM AS)	Part of the ITSQ report search results RFM Tab.	Yes	Name, beneficiaries' financial information, routing and account numbers. The privacy act records are covered by the OS-02, IIM Trust Funds SORN.
Trust Beneficiary Call Center (TBCC) Service Manager	Track and document beneficiary contact about trust assets or requests to update, or disburse funds from an IIM account.	Yes	Name, birth date, other names used, place of birth, SNN, cell/phone number, email address, mother's maiden name, mailing address, beneficiaries' financial information, routing and account numbers. Privacy Act records are covered by the OS-02, IIM Trust Funds SORN.