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: Tribal Enrollment Reporting and Payment System (TERPS)
Bureau/Office: Bureau of Indian Affairs (BIA), Office of Indian Services
Date: July 16, 2020
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd 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 Tribal Enrollment Reporting and Payment System (TERPS) is a commercial off-the-shelf (COTS), major application that functions as a central database for American Indian enrollment records, populated with records of Individual Indians who are applying for or have been assigned interests of any kind in Indian tribes, bands, pueblos or corporations, and individuals who are eligible to vote in Secretarial elections. TERPS' primary purpose is to assist the Bureau of Indian Affairs (BIA) to determine an individual's eligibility to share in judgment fund distributions authorized by plans prepared pursuant to 25 U.S.C. Section 1401, Funds

appropriated in satisfaction of judgments of Indian Claims Commission or United States Court of Federal Claims. It also assists BIA in calling and conducting Secretarial elections under 25 CFR Part 81, Tribal Reorganization under a Federal Statute.

C. What is the legal authority?

25 U.S.C. 1401, Funds appropriated in satisfaction of judgments of Indian Claims Commission or United States Court of Federal Claims; 25 U.S.C. Chapter 14, Subchapter XIX Shoshone and Arapaho Tribes of Wyoming; 25 CFR part 61, Preparation of Rolls of Indians; 25 CFR part 62, Enrollment Appeals; 25 CFR part 67, Preparation of a roll of independent Seminole Indians of Florida; 25 CFR part 75, Revision of the Membership Roll of the Eastern Band of Cherokee Indians, North Carolina; 25 CFR part 81, Tribal Reorganization under a Federal Statute; 25 CFR part 87, Use or Distribution of Indian Judgement Funds; 25 CFR part 90, Election of Officers of the Osage Tribe; 25 CFR Part 111, Annuity and other Per Capita Payments

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*

UII Code: 010-000000076, Tribal Enrollment Reporting and Payment System (TERPS), System Security Plan (SSP), March 24, 2020

☐ 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	Not Applicable	Not Application

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)*

Records in TERPS are maintained under DOI system of records notice BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 76 FR 59733, September 27, 2011, which

may be viewed at https://www.doi.gov/privacy/bia_notices. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1076-0153, Request for Certificate of Degree of Indian or Alaska Native Blood (CBID), Expires March 31, 2021

OMB Control Number 1076-0160, Verification of Indian Preference for Employment in the Bureau of Indian Affairs and the Indian Health Service, Expires March 31, 2021

OMB Control Number 1076-0183, Secretarial Elections, Expires February 28, 2022

☐ No

Section 2. Summary of System Data

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

☒ Name	☒ Social Security Number (SSN)	☒ Race/Ethnicity
☒ Gender	☒ Spouse Information	☒ Personal Cell Number
☒ Birth Date	☒ Financial Information	☒ Group Affiliation
☒ Personal Email Address	☒ Tribal or Other ID Number	☒ Marital Status
☒ Mother's Maiden Name	☒ Home Telephone Number	☒ Other Names Used
☒ Place of Birth	☒ Mailing/Home Address	☒ Military Status/Service
☒ Child or Dependent Information		
☒ Other:		

TERPS may contain documents supporting individual Indian claims to interests in Indian tribal groups and includes name, maiden name, alias, address, date of birth, social security number, blood degree, enrollment/BIA number, date of enrollment, enrollment status, certification by the tribal governing body, telephone number, e-mail address, account number, marriages, death notices, records of actions taken (approvals, rejections, appeals), rolls of approved individuals; records of actions taken (judgment distributions, per capita payments, shares of stock); ownership and census data taken using the rolls as a base, records concerning individuals which have arisen as a result of that individual's receipt of funds or income to which that individual was not entitled or the entitlement was exceeded in the distribution of such funds.

The Social Security Number is used to accurately identify individuals to ensure judgement distributions and per capita payments are correctly recorded and disbursed, to report taxes to the Department of the Treasury, and recover debts owed to the United States.

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*

Records are obtained from individual Indians who are applying for or have been assigned interests of any kind in Indian tribes, bands, pueblos or corporations, and individuals who register to vote in Secretarial elections. If the information is for a minor, the information is collected from parent or guardian. Records are also obtained directly from tribal governing bodies of Federally Recognized Indian Tribes. These tribes may submit enrollment information by tribal resolutions and code sheets. Commercial databases may be used to find the last known address of potential heirs, date of death, county of death, birth place, locate potential family relatives. Additional information on tribal enrollment and secretarial elections may come from internal DOI records.

C. How will the information be collected? Indicate all that apply.

- ☒ Paper Format
- ☒ Email
- ☒ Face-to-Face Contact
- ☐ Web site
- ☒ Fax
- ☒ Telephone Interview
- ☐ Information Shared Between Systems
- ☐ Other: *Describe*

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

PII collected is used to assist BIA in determining an individual's eligibility to share in judgment fund distributions authorized by plans prepared pursuant to 25 U.S.C. Section 1401, Funds appropriated in satisfaction of judgments of Indian Claims Commission or United States Court of Federal Claims. It also assists BIA in calling and conducting Secretarial elections under 25 CFR Part 81, Tribal Reorganization under a Federal Statute.

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.*

Information may be shared with BIA employees acting in their official capacity in the performance of official functions to determine eligibility to share in judgment fund distributions

and conduct Secretarial elections under 25 CFR Part 81, Tribal Reorganization under a Federal Statute.

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

Information may be shared with the Office of the Special Trustee for American Indians for the purpose of issuing checks related to judgment fund distributions and per capita payments.

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

Information may be shared with the Department of the Treasury to report taxes and recover debts owed to the United States, U.S. Department of Justice for litigation matters, and other Federal agencies as authorized pursuant to the routine uses contained in SORN BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 74 FR 59733, September 27, 2011, which may be viewed at https://www.doi.gov/privacy/bia_notices.

Information may be shared with representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906, as authorized pursuant to the routine uses contained in SORN BIA-07, Tribal Enrollment Reporting and Payment System (TERPS) system of records notice.

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

Information may be shared with the Tribe, Band, Pueblo or Corporation of which the individual to whom a record pertains is a member to confirm eligibility to vote in Secretarial Elections pursuant to 25 CFR Part 81, Tribal Reorganization under a Federal Statute; and as authorized pursuant to the routine uses contained in SORN BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 74 FR 59733, September 27, 2011.

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

Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support and as authorized pursuant to the routine uses contained in SORN BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 74 FR 59733, September 27, 2011.

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

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals do have the option of not providing information during a phone interview. But declining to provide information may affect their enrollment status or financial payments.

Individuals do have the option of not providing information requested by US mail by not returning the form, or by not responding to certain questions. But declining to provide information may affect their enrollment status or financial payments.

Individuals do have the option of not providing information when completing the Request for Certificate of Degree of Indian or Alaska Native Blood (CBID) (OMB 1076-0153). The information collected is used to determine eligibility of the individual to receive Federal program services. Providing the information is voluntary. Not providing the information could result in the BIA not being able to determine proof of Indian blood as required to receive Federal program services.

Individuals do have the option of not providing information when completing the Verification of Indian Preference for Employment in the Bureau of Indian Affairs and the Indian Health Service (Form BIA 5532)(OMB 1076-0160). The information collected is used to determine eligibility for preference when appointments are made to vacancies in positions in the Bureau of Indian Affairs. Providing the information is voluntary. Not providing the information could result in the BIA not being able to consider the individual for Indian preference in employment under 25 CFR part 5.

Individuals do have the option of not providing information when completing the Secretarial Elections form (OMB 1076-0183). The information collected is used to determine an Indian individual's eligibility to vote in a Secretarial election. Providing the information is voluntary. Failure to provide information could prevent the individual from participating in a Secretarial election.

☐ 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 provide to individuals on the Bureau of Indian Affairs Certificate of Degree of Indian or Alaska Native Blood, Verification of Indian Preference for Employment in the Bureau of Indian Affairs and the Indian Health Service forms, and the Secretarial Elections Form.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment and the published BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 76 FR 59733, September 27, 2011, which may be viewed at https://www.doi.gov/privacy/bia_notices. This

SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☒ 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.).

Records in TERPS are primarily retrieved by Name. Records may also be retrieved by any other keyword search such as Gender, Birth Date, Age, Marital Status, Other Names Used, Place of Birth, Spouse Information, Financial Information, Race/Ethnicity, Social Security Number (SSN), Personal Cell Telephone Number, Tribal ID, Other ID Number, Personal Email Address, Mother's Maiden Name, Home Telephone Number, Child or Dependent Information, Military Status/Service, Mailing/Home Address, Birth Family Information / Custody/Guardianship Information.

I. Will reports be produced on individuals?

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

Vital statistics reports on enrolled Tribal members are provided to Tribal Entities and BIA Program Offices; Registration lists for Tribal and Secretarial Elections are provided to Tribal Entities and BIA Tribal Government Services; and ancestry information for Tribal Enrollment services, to include the issuance of Identification Cards and /or Certificates of Degree of Indian Blood. Entities having access to the information include Tribal enrollment offices and DOI employees. Information may be provided to the Department of the Treasury for the issuance of checks.

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit Logs also collect information on system users such as username. System administrators and the information system owner have access to these activity reports.

☐ No

Section 3. Attributes of System Data

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

Applicants must certify that all the answers given are true, complete and accurate. Data collected from Tribal entities is certified by each tribe confirming that the listing is accurate and was created using their own tribal membership laws. Information gathered from other sources is crosschecked by Enrollment Specialists via certified legal documents.

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?

Applicants must certify that all the answers given are true, complete and accurate. Tribal entities and BIA Enrollment Specialists crosscheck information for completeness.

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).

Applicants must certify that all the answers given are true, complete and accurate. To ensure data is current, BIA Enrollment Specialists request updated tribal enrollment information from the Tribe or an individual tribal member before each Secretarial Election or distribution of funds.

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.

Paper records are covered by Indian Affairs Records Schedule (IARS) Records Series 3700 – Tribal Government under multiple file codes and have been scheduled as permanent records by the National Archives and Records Administration (NARA) under Job No. N1-075-05-0001, approved on March 31, 2005. Records may include lists of tribal members showing name, reservation, agency, sex, and degree of blood, residence, allotment status, and general docket numbers for tribal citizenship courts; records of births, marriage, per capita rolls, and death records. 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 in which tribal membership rolls are completed, when enrollments are updated, when enrollment periods are completed, when memberships are closed, and when per capita payments are disbursed to tribal members. 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 United States Department of the Interior and the National Archives and Records Administration.

A records retention schedule for the electronic records in this system is being developed and will be submitted to NARA for scheduling and approval. Pending approval by NARA, electronic records will be treated as permanent records.

TERPS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), 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.

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 TERPS is retained under the appropriate NARA approved Indian Affairs Records Schedules (IARS). 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 Office of the Special Trustee for American Indians, Office of Trust Records, records management policies and procedures. System administrators dispose of DOI records by shredding or pulping for paper records, and degaussing or erasing for electronic records in accordance with NARA Guidelines 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 a moderate risk to the privacy of individuals due to the sensitive PII contained in TERPS. TERPS 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. TERPS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 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.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. In an effort to protect the privacy of individuals, TERPS collects only the minimal amount of information needed to perform official functions for which the system was designed. Users are also advised not to share or publish sensitive data and the system administrators periodically review user accounts to ensure compliance with access requirements. To mitigate this risk, access to files is strictly limited to authorized personnel who require access to perform their official duties. BIA manages TERPS 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 TERPS user accounts. In addition to physical controls, operational and technical controls in

place to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users. System administrators utilize user identification, passwords, "least privileges," 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. Access controls and system logs are reviewed regularly as part of the continuous monitoring program.

There is a risk that TERPS 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. To mitigate this risk, access to data is restricted and authorized personnel are instructed to not gather or store unnecessary information about individuals. Access controls are implemented to ensure only authorized personnel have access to the information needed to perform official duties and access to TERPS is limited to Division of Tribal Government Services employees and contractors. 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. 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. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification and periodic verification of system users. Firewalls and intrusion detection systems monitor and block unauthorized connections. Current antivirus software is used to check for viruses in real time and logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest, when stored on Federal government owned and operated computer systems with restricted access. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use. TERPS meets BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. This risk is mitigated through established quality control procedures to check the completeness and accuracy of information before entering data into TERPS. Data collected from Tribal entities is certified by each tribe confirming that the information is accurate and was created using their own tribal membership laws. Information gathered from other sources is crosschecked by Enrollment Specialists via certified legal documents. Additionally, BIA Enrollment Specialists request updated tribal enrollment information from the Tribe or an individual tribal member before each Secretarial Election or distribution of funds.

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. In regards to information handling and retention procedures, the Division of Tribal Government Services is

responsible for managing and disposing of BIA records in TERPS 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 Tribal Government Services ensures only records needed to support its program, Tribes, and Tribal members is maintained. The Division of Tribal Government Services maintains the records in the office of record 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 (AIRR), a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code No. N1-075-05-0001, approved on March 31, 2005. Information collected and stored within TERPS 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. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published SORN, BIA-07, Tribal Enrollment Reporting and Payment System (TERPS), 76 FR 59733, September 27, 2011, which may be viewed at: https://www.doi.gov/privacy/sorn. Additionally, Privacy Act Statements (PAS) are part of the Request for Certificate of Degree of Indian or Alaska Native Blood (CBID), the Verification of Indian Preference for Employment in the Bureau of Indian Affairs and the Indian Health Service, and the Secretarial Elections form. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

An audit trail of activity is maintained 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 SP 800-53 Revision 4, 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 upon employment and annually thereafter, to ensure an understanding of their 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 the system and information collected is relevant and necessary to the purpose for which TERPS was designed, which is to assist the BIA in collecting data to determine an Indian individual's eligibility to share in judgment fund distributions authorized by plans prepared pursuant to 25 U.S.C. Section 1401, Funds appropriated in satisfaction of judgments of Indian Claims Commission or United States Court of Federal Claims. It also assists BIA in calling and conducting Secretarial elections under 25 CFR part 81, Tribal Reorganization under a Federal Statute.

☐ 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. TERPS 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: *Describe*

Access to information is limited to those authorized individuals that have a "need-to-know" in order to perform official duties, including system administrators, authorized program personnel, and contractors based on the "least privilege" principle. Contractors may be involved in the design and development of TERPS, or with maintenance of the system, and may support tribal enrollment functions and processes managed by TERPS. System Administrators have access to TERPS in the performance of their official functions. The activities of System Administrators are logged and audited.

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

The Information System Owner, system manager, program manager, and supervisors determine user access based on the role and duties of the individual. Users are only given access to data on a "least privilege" principle and "need-to-know" to perform official functions. BIA manages TERPS 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 TERPS 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.

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 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 following Privacy Act contract clauses were included in the contract.

- 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 TERPS is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system.

☐ No

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

The TERPS system is not intended to monitor individuals; however the system has the functionality to audit user activity. 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. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

TERPS has the ability to 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 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring. TERPS 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. TERPS 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 will be required to consent to TERPS 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 TERPS 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.

- [x] Security Guards
- [x] Key Guards
- [x] Locked File Cabinets
- [x] Secured Facility
- [x] Closed Circuit Television
- [ ] Cipher Locks
- [x] Identification Badges
- [ ] Safes
- [ ] Combination Locks
- [x] Locked Offices
- [ ] Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- [x] Password
- [x] Firewall
- [x] Encryption
- [x] User Identification
- [ ] Biometrics
- [x] Intrusion Detection System (IDS)
- [x] Virtual Private Network (VPN)
- [x] Public Key Infrastructure (PKI) Certificates
- [x] Personal Identity Verification (PIV) Card
- [ ] Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- [x] Periodic Security Audits
- [x] Backups Secured Off-site
- [x] Rules of Behavior
- [x] Role-Based Training
- [x] Regular Monitoring of Users' Security Practices
- [x] Methods to Ensure Only Authorized Personnel Have Access to PII
- [x] Encryption of Backups Containing Sensitive Data
- [x] 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 Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office 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, used and stored in TERPS. The ISO and the Privacy Act system managers are

responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the 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 TERPS ISO and ISSO are responsible for the central oversight and management of the TERPS 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 TERPS ISO, ISSO, and bureau and office system administrators 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 DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials. 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.