



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our [Privacy Office Support Request Page](#). For further guidance, consult the [DOI PIA Guide](#).

System Information

System or Project Name:	Progeny-Tribal Enrollment Reporting and Payment System
System or Project Acronym:	TERPS/Progeny
Bureau or Office:	BIA
Date Signed:	June 30, 2026
System Operational Status:	Modification

Point of Contact

Name:	Constance Sue Sheffer
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

- | | |
|--|---|
| ☐ New System | ☐ Significant Modification |
| ☐ New Electronic Collection | ☒ Other: Describe below |

This PIA is being updated as part of the Department's periodic privacy review process to ensure that the assessment remains current and accurate. The update also consolidates the previously separate TERPS and Progeny privacy assessments because the applications operate within the same authorized system boundary. This consolidation does not, by itself, represent a new collection of PII.

2. What is the purpose of the system or project?

Progeny and the Tribal Enrollment Reporting and Payment System (TERPS) are applications within a common BIA system boundary that support tribal enrollment, eligibility, Secretarial election, and payment-related

functions.

Progeny is a commercial off-the-shelf application used by BIA to manage and verify American Indian and Alaska Native enrollment information. Progeny supports region-specific enrollment databases, including Alaska, California, and Western Shoshone records, and provides functionality for enrollment searches, lineage and descendency management, and preparation of Certificates of Degree of Indian or Alaska Native Blood (CDIB).

TERPS supports BIA's centralized tribal enrollment reporting, judgment fund distribution, per capita payment, and Secretarial election functions. It maintains records concerning individuals applying for or assigned interests in tribes, bands, pueblos, or corporations and individuals whose information is used in authorized Secretarial election activities.

3. Is the system registered in BisonGRC?

- ☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

The system is registered in BisonGRC under UII Code 010-000000076. The Tribal Enrollment Reporting and Payment System (TERPS) is documented in the System Security Plan (SSP), and Progeny – Tribal Enrollment System in Alaska is documented in the System Security and Privacy Plan (SSPP). Both are maintained under the same UII because they operate within the same system boundary.

4. What legal authorities authorize the collection and use of data in this system or project?

The collection and use of data in Progeny is authorized by the following federal statutes and regulations governing tribal enrollment, judgment fund distributions, Secretarial elections, per capita payments, and related eligibility determinations:

- 25 U.S.C. § 1401 – Funds appropriated in satisfaction of judgments of Indian Claims Commission and United States Court of Federal Claims
- 25 U.S.C. Chapter 14, Subchapter XLVII – Shoshone and Arapaho Tribes of Wyoming
- 25 CFR Part 61 – Enrollment Appeals
- 25 CFR Part 62 – Preparation of Rolls of Indians
- 25 CFR Part 67 – Preparation of a Roll of Independent Seminole Indians of Florida
- 25 CFR Part 76 – 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 Judgment Funds
- 25 CFR Part 90 – Election of Officers of the Osage Tribe
- 25 CFR Part 111 – Annuity and Other Per Capita Payments

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

- ☒ Yes: If yes, list the applicable citations below.
☐ No

Records maintained in TERPS and Progeny are covered by INTERIOR/BIA-7, Tribal Enrollment Reporting and

Payment System, 76 FR 59733 (September 27, 2011), as subsequently modified.

The SORN covers records maintained in support of tribal enrollment, eligibility, Secretarial elections, judgment fund distributions, per capita payments, and related authorized BIA functions.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

- ☒ Yes
☐ No

OMB Control Number 1076-0153 – Request for Certificate of Degree of Indian or Alaska Native Blood (CDIB), expires April 30, 2029.

OMB Control Number 1076-0160 – Verification of Indian Preference for Employment in the Bureau of Indian Affairs and the Indian Health Service, expires December 31, 2028.

OMB Control Number 1076-0183 – Secretarial Elections, expires April 30, 2029.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

Progeny and TERPS operate within the same system boundary under UII Code 010-000000076. Progeny-Tribal Enrollment System in Alaska is a region-specific database within Progeny that supports the management and verification of Alaska Native tribal enrollment records. It processes tribal enrollment information, identifying information, lineage and descendency records, and related eligibility documentation.

Progeny – Tribal Enrollment System in Alaska: A regional database within Progeny that supports the management and verification of Alaska Native tribal enrollment records. It processes tribal enrollment information, identifying information, lineage and descendency records, and related eligibility documentation.

Tribal Enrollment Reporting and Payment System (TERPS): The desktop application that supports tribal enrollment reporting, judgment fund distributions, Secretarial elections, and related eligibility determinations. It processes enrollment, payment, and eligibility information containing personally identifiable information (PII).

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

- | | | |
|--|---|---|
| ☒ Name (full, first or last) | ☒ Home telephone number | ☐ Employment or resume info |
| ☒ Aliases/nickname | ☒ Personal Email | ☒ Full or Truncated SSN |
| ☐ Driver's license | ☒ Mailing or home address | ☐ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☐ Biometrics/facial recognition |
| ☐ Legal Status | ☒ Mother's maiden name | ☐ Vehicle information |
| ☒ Sex | ☒ Marital status | ☐ Passport information |
| ☒ Race or ethnicity | ☒ Spouse Information | ☐ Travel information |
| ☒ Date of birth | ☒ Child or family information | ☒ Parent's name |
| ☒ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☒ Personal cell phone number | ☒ Financial information | ☐ Nationality |

- | | | |
|--|---|---|
| ☒ Username / user ID / acct ID | ☒ IP address / network ID | ☒ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☐ Photos / video / audio | ☐ Health / medical information |
| ☒ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Criminal / disciplinary info | ☒ Military records | ☒ Other: Describe below |

TERPS/Progeny maintains PII necessary to support authorized tribal enrollment, lineage and descendancy, eligibility, Secretarial election, judgment fund distribution, and related program functions.

Information may include name, maiden name, aliases, mailing and residential address, date and place of birth, Social Security number, blood degree, tribal or BIA enrollment number, enrollment status, telephone number, email address, marital and spouse information, parent and family or lineage information, financial and payment-related information, military information, and documentation concerning enrollment actions, appeals, distributions, and other authorized program actions.

The system also maintains user identifiers and audit information associated with authorized system access and activity.

2. What is the source for the PII collected? Check all that apply.

- | | |
|---|--|
| ☒ Individual | ☒ DOI Records |
| ☐ Federal Agency | ☒ Third Party Records |
| ☒ Tribal Agency | ☐ State Agency |
| ☐ Local Agency | ☒ Other: <i>Describe Below</i> |

Records are obtained from individuals, parents or guardians acting for minors, authorized representatives, federally recognized Tribal governments, DOI records, and other authorized sources supporting tribal enrollment and related program functions.

Tribal governments may provide enrollment information through official tribal rolls, resolutions, code sheets, and supporting documentation.

Commercial third-party databases may also be used for limited program purposes such as locating individuals or potential heirs and verifying address, death, birthplace, or family-location information. Information obtained from those sources is subject to program validation before it is relied upon for an official determination.

3. How will the information be collected? Check all that apply.

- | | |
|--|--|
| ☒ Paper Format | ☒ Fax |
| ☒ Email | ☒ Telephone Interview |
| ☒ Face-to-Face Contact | ☐ Shared Between Systems: <i>Describe</i> |
| ☐ Website | ☐ Other: <i>Describe</i> |

Information is collected as part of the Tribal enrollment and certification process through enrollment applications and supporting documentation submitted by individuals or their authorized representatives, Tribal governments, and Bureau of Indian Affairs (BIA) offices. The information is derived from official tribal rolls, lineage and descendancy documentation, and related eligibility records, and is entered and maintained in the system by authorized personnel to support enrollment tracking, certification, and eligibility determinations.

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

PII maintained in TERPS/Progeny is used to administer authorized BIA tribal enrollment and related functions, including maintaining tribal enrollment records and rolls; verifying identity, lineage, descendency, blood degree, and membership-related information; issuing Certificates of Degree of Indian or Alaska Native Blood (CDIB); processing enrollment appeals; determining eligibility for judgment fund distributions and per capita payments; supporting Secretarial elections; and performing related authorized program and reporting activities.

5. How does this project limit the collection and use of PII to only what is necessary?

TERPS/Progeny limits the collection and use of PII to information necessary to perform authorized tribal enrollment, lineage and descendency verification, CDIB, election, judgment fund distribution, per capita payment, appeal, and related program functions.

BIA collects only the identifying, family, tribal affiliation, eligibility, payment, and supporting information necessary for the specific program activity being performed. Information submitted by individuals, Tribal governments, or other sources is reviewed by authorized program personnel before it is entered into or relied upon in the system.

Access to PII is further restricted through role-based access controls, least privilege, and need-to-know requirements.

Section 3: Data Sharing and Individual Rights

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

- ☒ **Within the Bureau/Office:** Describe how the data will be used below.
- ☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
- ☒ **Other Bureaus/Offices:** Describe how the data will be used below.
- ☒ **Contractor:** Describe how the data will be used below.
- ☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
- ☐ **Other Third-Party Sources:** Describe how the data will be used below.

Within BIA: Information is shared with authorized BIA personnel as necessary to perform tribal enrollment, CDIB, Secretarial election, judgment distribution, appeal, and related official functions.

Tribal governments: Information may be shared with the applicable Tribe, Band, Pueblo, or other authorized Tribal entity for enrollment administration, eligibility confirmation, election administration, and other authorized program purposes consistent with INTERIOR/BIA-7.

Other DOI bureaus/offices: Information may be shared with BTFA and other authorized DOI components when necessary to perform payment, trust administration, or related official functions.

Contractors: Authorized contractors providing system maintenance, development, administration, or technical support may access information necessary to perform assigned duties subject to applicable contract, Privacy Act, security, training, and access-control requirements.

Other Federal agencies: Information may be shared with the Department of the Treasury and other authorized Federal agencies for payment, tax, integrity, or other purposes described in applicable law and INTERIOR/BIA-7..

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

- ☐ Yes
☒ No

No. A separate MOU, MOA, or ISA is not required because the information sharing is governed by applicable federal statutes and regulations, the Privacy Act of 1974, the published System of Records Notice (SORN), INTERIOR/BIA-7 – Indian Enrollment Records, and applicable contracts.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

- ☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals may decline to provide information during phone interviews, by mail, or when completing forms such as the CDIB, Verification of Indian Preference, or Secretarial Election documents. However, because this information is used to determine eligibility for Federal services, employment preference, or participation in Secretarial elections, choosing not to provide it may prevent the Bureau of Indian Affairs from verifying eligibility or processing benefits.

Individuals must provide information when completing the Secretarial Elections form. The information collected is used to determine an Indian individual's eligibility to vote in a Secretarial election. While providing the information is voluntary, failure to provide information could prevent the individual from participating in a Secretarial election

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

- ☒ Privacy Act Statement: ☒ Other: *Describe Below*
☒ Privacy Notice: ☐ None: *Example - law enforcement cases.*

A Privacy Act Statement is provided to individuals on the BIA Request for Certificate of Degree of Indian or Alaska Native Blood (CDIB), Verification of Indian Preference for Employment in BIA and IHS form, and the Secretarial Elections form.

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, as amended.

Other: 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.

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

Authorized users may retrieve enrollment and related records using identifiers and search fields maintained in the system, including name, Social Security number, date of birth, tribal or enrollment identifier, other assigned identifier, address, telephone number, email address, family or lineage information, and other authorized program search criteria.

Retrieval capabilities are restricted to authorized users based on assigned role, need-to-know, and program responsibility.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.

☐ No

Yes. Reports containing PII are produced only for authorized program purposes.

Vital statistics reports are provided to Tribal entities and authorized BIA Program Offices to support tribal enrollment administration.

Registration lists are provided to Tribal entities and BIA Tribal Government Services to administer Tribal and Secretarial elections.

Ancestry reports are provided to authorized Tribal enrollment offices and DOI employees to support tribal enrollment services, including issuance of Identification Cards and Certificates of Degree of Indian Blood (CDIB).

Payment-related information may be provided to the Department of the Treasury for issuance of judgment funds and per capita payments, as authorized.

Audit log reports are available only to authorized system administrators and the Information System Owner for security monitoring, auditing, and incident investigation.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Tribal enrollment and related program records maintained in TERPS/Progeny are retained in accordance with the NARA-approved disposition authority applicable to the Indian Affairs tribal enrollment record series.

Records designated as permanent are preserved and transferred in accordance with the applicable NARA-approved schedule and DOI/Indian Affairs records-management procedures. Paper records are transferred from

the office of record to the designated Federal records repository in accordance with approved disposition instructions.

Electronic records are retained and transferred in accordance with the disposition authority applicable to the electronic recordkeeping copy. Backup copies are managed separately under the disposition authority applicable to backup and system-recovery records.

2. What measures are used to maintain the accuracy and completeness of data received from external sources after receipt and throughout the records lifecycle?

- ☒ External-source data is received and validated as described below
☐ N/A: The system does not receive data from sources other than DOI records

Data received from external sources, such as individuals, authorized representatives, or tribal governments, is reviewed by authorized Bureau of Indian Affairs personnel before being entered into or updated in the system. Information is compared against official tribal rolls, enrollment applications, lineage and descendency documentation, and existing BIA records to confirm identity and membership status. Only authorized users may update records, and system activity is logged and audited to ensure accountability. These administrative reviews, access controls, and audit mechanisms help validate the accuracy and completeness of the data maintained in the system

Records are updated as new or corrected information becomes available through authorized program processes, and all changes are subject to established review procedures, role-based access controls, and audit logging to help maintain the ongoing accuracy and integrity of the information throughout its lifecycle.

3. Does the project include logging capabilities to record and monitor access to PII?

- ☒ Yes
☐ No

The system maintains an audit trail that records user activity, including:

- Username
- Logon date and time
- Number of failed login attempts
- Files accessed
- User actions or changes made to records

Audit logs are reviewed on a regular basis, and any suspected unauthorized access or improper use is reported to IT Security. System Administrators review system usage to ensure the system is not improperly used and to prevent unauthorized access.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

Risk: There is a risk that inaccurate, incomplete, or excessive personal information could be collected during the tribal enrollment process.

- **Mitigation:** Information is collected under specific statutory and regulatory authorities governing tribal enrollment and related functions. Authorized BIA personnel review enrollment applications and support documentation before information is entered into the system. Data is limited to what is necessary to verify identity, lineage, descendency, and eligibility for services and distributions. Access to enter or modify information is restricted to authorized users with a need-to-know.

Risk: There is a risk that PII could be used for purposes other than those authorized under federal law.

- **Mitigation:** PII is used only for official tribal enrollment functions, including maintaining tribal rolls, verifying membership, issuing Certificates of Degree of Indian Blood (CDIB), processing enrollment appeals, and determining eligibility for services, judgment funds, and per capita payments. System access is role-based and follows the least privilege principle. All users must complete privacy and security training before being granted access

Risk: There is a risk of retaining information longer than necessary or failing to properly protect long-term records.

- **Mitigation:** Records are maintained in accordance with approved National Archives and Records Administration (NARA) records schedules applicable to tribal enrollment records. These records are treated as long-term or permanent due to their importance in documenting tribal membership and lineage. Records are retired and transferred according to DOI and NARA procedures.

Risk: There is a risk of unauthorized access, internal misuse, or unauthorized disclosure of sensitive personally identifiable information (PII), including Social Security Numbers, tribal enrollment information, and other sensitive records maintained by the system

- **Mitigation:** The system is categorized as a FISMA Moderate system and implements NIST Special Publication 800-53 security and privacy controls to protect sensitive PII. Access is restricted through role-based access controls and the principles of least privilege and need-to-know. Before being granted access, users must complete mandatory security, privacy, and records management training and acknowledge the DOI Rules of Behavior to ensure they understand their responsibility to safeguard sensitive information and individual privacy. Authorized personnel are instructed not to collect, use, or retain information beyond what is necessary to perform their official duties. Additional safeguards include audit logging of user activity, monitoring of login attempts and system actions, firewall and network security configurations, annual security and privacy awareness training, and controlled access to facilities and locked offices. Audit logs are reviewed regularly, and any suspected unauthorized access or improper use is reported to IT Security.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

- ☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
- ☒ No

TERPS/Progeny does not generate new predictive, scored, inferred, or analytically derived information about individuals through aggregation or automated analytics. The system maintains submitted and verified enrollment, lineage, eligibility, payment, and supporting information.

Authorized BIA personnel use those records to make program determinations under applicable statutory and regulatory authorities. Those determinations are based on the underlying records and established program criteria rather than newly generated analytical inferences.

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

- ☐ Yes: *Provide explanation below*
☒ No

TN/A. TERPS/Progeny does not generate the new or inferred data described in Question 2.

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

- ☐ Yes: *Provide explanation below*
☒ No

ERPS/Progeny does not make additional determinations based on newly generated or analytically inferred data. Authorized BIA personnel make enrollment, CDIB, election, appeal, judgment distribution, and other authorized eligibility determinations using submitted and verified records and established program criteria.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

N/A.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

- ☐ Yes
☒ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

Not applicable. Progeny Tribal Enrollment System in Alaska and TERPS do not use AI, machine learning, or analytical models.

3. Are individuals notified of AI-based decisions that affect them?

- ☐ Yes
☒ No

Not applicable. Progeny – Tribal Enrollment System in Alaska and TERPS do not make or support AI-based decisions about individuals.

4. Are safeguards in place to prevent bias or unintended consequences?

- ☐ Yes
☒ No

Not applicable. Progeny Tribal Enrollment System in Alaska and TERPS do not use AI or model-driven capabilities that could introduce model bias or AI-specific unintended consequences.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

- ☐ Yes
☒ No

Not applicable. Progeny Tribal Enrollment System in Alaska and TERPS do not use AI or analytical models requiring periodic review or retraining.

6. Is federated learning used for privacy-preserving model training?

- ☐ Yes
☒ No

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

- | | |
|---|--|
| ☒ Users | ☒ System Administrator |
| ☒ Contractors | ☒ Other: <i>Describe below</i> |
| ☐ Developers | |

Access is limited to authorized Bureau of Indian Affairs (BIA) personnel, system administrators, and authorized contractors who require access to perform official duties. Access is granted based on documented need and principle of least privilege.

User access is role-based and determined by job responsibilities. Supervisors and system managers approve access requests. System administrators manage account creation, modification, and removal in accordance with DOI policy. Users must:

- Complete required DOI security and privacy training
- Acknowledge DOI Rules of Behavior
- Use authenticated credentials to access the system

Contractors must sign nondisclosure agreements as a condition of 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).

2. What data protection policies apply to cloud-based PII storage?

N/A

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The system includes audit logging and monitoring capabilities and maintains audit trails that record:

- Username
- Logon date and time
- Failed Login attempts
- Files accessed

Audit logs are reviewed regularly by system administrators. Any suspected unauthorized access or unusual activity is reported to DOI IT Security for investigation.

Additional safeguards include:

- Firewalls and network security controls
- Intrusion detection and monitoring consistent with DOI security policy
- Enforcement of least privileged access
- Separation of duties
- Continuous monitoring consistent with FISMA Moderate requirements
- Required completion of Annual Information Management and Technology Awareness Training

These monitoring and detection controls help identify, contain, and mitigate unauthorized access or attempted data exfiltration.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

- ☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
- ☐ No

The system includes monitoring of user activity for security and accountability purposes. It maintains audit logs that record user login information, failed login attempts, files accessed, and actions taken within the system. These logs are reviewed regularly by system administrators to detect unauthorized access or misuse. Monitoring is limited to system usage and security oversight and is not used to monitor individuals for surveillance purposes or to track individuals beyond maintaining official enrollment records. Monitoring is conducted solely to protect the integrity, confidentiality, and availability of the information maintained by the system.

Controls ensuring appropriate use of monitoring capabilities include:

- Role-based access controls
- Least privilege and need-to-know access
- Separation of duties
- DOI Rules of Behavior acknowledgment

- Required annual privacy and security training
- Regular audit log review
- Reporting of suspected incidents to DOI IT Security

These safeguards ensure monitoring capabilities are used only by authorized personnel for approved security and oversight purposes.

5. Will contractors be involved in the following project activities? Check all that apply.

- ☒ Design
- ☒ Development
- ☒ Maintenance

Authorized contractors may be involved in the design, development, and maintenance of the system, including providing technical support and system administration services. Contractors must comply with DOI security and privacy requirements before being granted access. Requirements include:

Completing DOI security and privacy awareness training

- Signing DOI Rules of Behavior
- Operating under role-based access controls and least privileged principles
- Complying with Federal Information Security Modernization Act (FISMA) requirements
- Being subject to audit logging and monitoring
- Following applicable federal privacy and security standards (e.g., NIST SP 800-53 controls)

Contractor access is limited to official duties and is subject to the same oversight and monitoring as government personnel.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

- | | |
|--|---|
| ☒ Security Guards | ☐ Cipher Locks |
| ☒ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☐ Safes |
| ☒ Secured Facility | ☐ Combination Lock |
| ☐ Closed Circuit Television | ☐ Other: <i>Describe Below</i> |

The system is categorized as a FISMA Moderate system and implements security and privacy controls consistent with NIST SP 800-53 and DOI security policies.

Physical safeguards protect facilities and paper records through secured buildings, locked offices, identification badges, and monitored access controls.

Technical Controls

- | | |
|--|--|
| ☒ Password | ☒ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☒ Virtual Private Network (VPN) |
| ☒ Encryption | ☒ Public Key Infrastructure (PKI) Certificates |

- ☒ User Identification
☐ Other: *Describe Below*

☐ Biometrics

Describe the other types of controls implemented.

Administrative Controls

- | | |
|--|---|
| ☒ Periodic Security Audits | ☒ Methods to Ensure Only Authorized Personnel Have Access |
| ☒ Backups Secured Off-site | ☒ Encryption of Backups Containing Sensitive Data |
| ☒ Rules of Behavior | ☒ Mandatory Security, Records and Privacy Training |
| ☒ Role-Based Training | ☒ Regular Monitoring of Users' Security Practices |
| ☒ Other: <i>Describe Below</i> | |

Rules of behavior, separation of duties and Privacy and Record Management Training.

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals may submit a Privacy Act complaint concerning Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS) to the DOI Privacy Office. Complaints are logged, reviewed, and addressed in accordance with DOI privacy policies and procedures. Current contact information is available on DOI's public privacy website.

8. What processes are in place for individuals to access their information?

Individuals seeking access to records about themselves maintained by Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS) may submit a written Privacy Act request to the appropriate DOI Privacy Act Officer in accordance with 43 CFR Part 2, Subpart K. DOI verifies the requester's identity before releasing records.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking correction or amendment of records about themselves maintained by Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS) may submit a written Privacy Act amendment request to the appropriate DOI Privacy Act Officer in accordance with 43 CFR Part 2, Subpart K. DOI reviews the request and notifies the individual of the determination.

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

The System Owner for Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS) is responsible for ensuring proper use of the data and limiting access to authorized users with an official need to know. All authorized users must immediately report any suspected or confirmed loss, compromise, unauthorized disclosure, or unauthorized access involving personally identifiable information (PII) to DOI-CIRC and the Department Privacy Office in accordance with DOI policy.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a suspected or confirmed privacy breach involving Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS), DOI will immediately report the incident to DOI-CIRC and the Department Privacy Office; contain the incident; preserve relevant evidence; assess the nature, scope, and risk of harm; and implement appropriate mitigation. DOI will notify affected individuals and applicable oversight entities when required by law, policy, and the incident risk assessment.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

Progeny – Tribal Enrollment System in Alaska and the Tribal Enrollment Reporting and Payment System (TERPS) will be reviewed annually through the Privacy Threshold Analysis process and whenever a significant change to the system, data, technology, sharing, or operations may affect privacy risk. The PIA will be updated when the review identifies a material change affecting the accuracy, scope, or legal sufficiency of the assessment.

.