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:	eNativeTrust
System or Project Acronym:	ENT
Date submitted for review:	March 18, 2026
System Operational Status:	Development

Point of Contact

Name:	Dianna Taylor
Title:	Privacy Officer
Office:	OCIO
Phone:	703-787-1763
E-mail:	dianna_taylor@ios.doi.gov

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 conducted due to the development and planned deployment of the eNativeTrust System (ENT), a new system that will collect, maintain, and process personally identifiable information (PII) in support of probate case preparation, adjudication, and trust asset distribution. ENT introduces new capabilities, including electronic submission of probate documents, centralized case management, and AI-assisted document review to support staff in organizing and processing case materials. These capabilities create new privacy considerations related to the collection, use, and handling of sensitive PII within probate workflows. This PIA is conducted to assess these capabilities and ensure compliance with the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and applicable Department of the Interior privacy policies and governance requirements.

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

The eNativeTrust System (ENT) supports the Bureau of Indian Affairs (BIA) mission by enabling the preparation, submission, processing, and tracking of probate case records and related trust asset information. The system supports probate activities involving trust or restricted land and associated assets, helping ensure that estates are accurately reviewed and distributed in accordance with applicable laws and regulations.

ENT is a cloud-based system that provides a centralized environment for managing probate case information. It is used by authorized personnel across BIA, the Office of Hearings and Appeals (OHA), the Land Titles and Records Office (LTRO), the Bureau of Trust Funds Administration (BTFA), tribal governments, and authorized representatives who participate in probate workflows.

The system supports key functions such as case management, document submission and review, and coordination across offices involved in probate processing. ENT allows users to securely submit, store, and review probate-related documents, including wills, vital records, and other supporting materials required to establish heirship and process estates.

ENT improves the efficiency, consistency, and timeliness of probate case preparation by reducing manual processes, minimizing duplication, and supporting more effective coordination among participating offices. The system also includes limited AI-assisted functionality to help users identify required documentation and assess completeness of case materials. These capabilities are advisory in nature and require human review and validation prior to use.

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 eNativeTrust System (ENT) is not yet registered in BisonGRC because it is currently undergoing development and initial privacy and security documentation. BisonGRC registration will be completed as part of the Authorization and Assessment (A&A) process prior to obtaining an Authority to Operate (ATO) and deployment to a production environment.

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

The eNativeTrust System (ENT) operates under authorities governing Indian probate, trust asset administration, and federal privacy compliance. These authorities establish the legal basis for the collection, use, and management of personally identifiable information (PII) within the system.

- **The American Indian Probate Reform Act (AIPRA), 25 U.S.C. § 2201 et seq., and The American Indian Trust Fund Management Reform Act of 1994, 25 U.S.C. § 4001 et seq.,** - together govern the probate and distribution of trust land and Individual Indian Money (IIM) accounts. This is relevant because ENT supports the processing and coordination of probate-related trust asset distributions.
- **Title 25 CFR Part 15, "Probate of Indian Estates,"** - establishes regulatory procedures for probate case processing. This is relevant because ENT supports the intake, review, and management of probate case records in accordance with these requirements.
- **Title 43 CFR Part 30, "Indian Probate Hearings Procedures,"** - governs hearings and adjudication processes conducted by the Office of Hearings and Appeals (OHA). This is relevant because ENT supports workflows that interface with probate adjudication processes.

- **The Privacy Act of 1974, 5 U.S.C. § 552a, -** establishes requirements for the collection, maintenance, use, and dissemination of PII by federal agencies, including requirements for System of Records Notices (SORNs), access, and safeguarding of records. This is relevant because ENT maintains records that are retrieved by personal identifiers and must comply with Privacy Act requirements**.**
- **The E-Government Act of 2002, Section 208, -** requires federal agencies to conduct Privacy Impact Assessments (PIAs) for systems that collect, maintain, or disseminate PII. This is relevant because ENT collects and processes PII in support of probate operations, requiring evaluation of privacy risks and protections
- **OMB Circular A-130, "Managing Information as a Strategic Resource,**" - establishes federal policy for information governance, including privacy, security, and risk management requirements. This is relevant because ENT must ensure the proper safeguarding and management of PII in accordance with federal standards.
- **Departmental Manual (DM) 383, "Privacy Act Policy and Responsibilities**,"- implements DOI's internal privacy framework, including roles, responsibilities, and requirements for handling PII. This is relevant because ENT is subject to DOI privacy policy and oversight.

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

The Electronic Probate System (EPS) requires coverage under the Privacy Act, as records are retrieved by personal identifiers, including name, tribal enrollment number, address, date of birth, date of death, and case number.
The applicable SORN framework is currently in transition. At present, EPS aligns with the following notices:

- **INTERIOR/BIA–27, Bureau of Indian Affairs Probate Files**, 72 FR 8767 (February 27, 2007); modification published 86 FR 50156 (September 7, 2021), which historically covers probate case records, including information on decedents, heirs, and related documentation.
- **INTERIOR/BIA–04, Trust Asset and Accounting Management System (TAAMS)**, 79 FR 68292 (November 14, 2014); modification published 86 FR 50156 (September 7, 2021), which covers trust asset ownership and management of Individual Indian Money (IIM) accounts.

Consistent with current Departmental efforts, BIA-27 is being consolidated into an amended BIA-04 SORN to provide a unified framework for probate and trust-related records. As such, BIA-27 should be understood as providing transitional coverage pending completion of the updated BIA-04 notice.
EPS data elements and retrieval practices align with the categories described in these notices; however, the amended BIA-04 SORN will be required to fully reflect current system functionality, including AI-enabled processing activities such as document classification, summarization, and inference

The Electronic Probate System (EPS) requires coverage under the Privacy Act, as records are retrieved by personal identifiers, including name, tribal enrollment number, address, date of birth, date of death, and case number.

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

☒ Yes
☐ No

ENT includes or interfaces with information collections associated with existing PRA-approved DOI forms and workflows, including OMB Control No. 1076-0169, Probate of Indian Estates (OHA-7). Consistent with the approved PTA determination, coordination with the Information Collection Clearance Officer is required to confirm whether the Tribal Family Portal and any new or modified electronic intake workflows are fully covered by existing approvals or whether a revision or additional PRA clearance is required.

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

The eNativeTrust System (ENT) hosts the following minor applications and subsystems that are covered under this PIA:

- **eProbate Core-**The primary case-management and data-processing system that stores finalized probate data, manages workflows, and orchestrates interactions with all other eNativeTrust components.
- **Document Enrichment Engine (OCR/AI)-**The Document Enrichment Engine performs OCR and AI-based data extraction, supports Human-in-the-Loop review, and returns validated structured data to the eProbate Core.
- **GreenRoom Model Training Environment-**The manually invoked AI model-training platform used for dataset preparation, annotation review, experiment tracking, and batch model generation.
- **Cognitive Analytics Platform-** Provides downstream analytics and AI workloads by processing exported probate data for reporting, insights, and advanced modeling.

These subsystems are integral to ENT operations and share the same security, access control, and privacy safeguards described in this PIA.

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

The eNativeTrust System (ENT) collects, uses, and stores the following categories of personally identifiable information (PII) for members of the public, including decedents, heirs, beneficiaries, and authorized representatives, as well as limited PII for federal employees and contractors who access the system.

- Full Name (including aliases, if applicable) – Used to identify individuals involved in probate cases and associate individuals with specific case records and documentation.
- Date of Birth and Date of Death – Used to verify identity, establish heirship, and support probate case processing and adjudication.
- Sex and Marital Status – Used to support identity verification and establish family relationships relevant probate determinations.
- Race or Ethnicity / Tribal Affiliation – Used to support identification and determine eligibility for trust asset distribution and probate processing.
- Mailing or Home Address – Used for official correspondence, notifications, and communication related to probate proceedings.
- Personal Email Address and Telephone Numbers (including home and mobile) – Used to communicate with individuals regarding case status, required documentation, and submission follow-up.
- Username / user ID / acct ID – Used to identify Tribal Member and Tribal Family login.gov accounts.
- Tribal Enrollment Number or Tribal Identification – Used to verify identity and determine eligibility for probate and trust asset distribution.
- Family and Kinship Information (including Parent Names, Spouse Information, and Child or Family Relationships) – Used to establish relationships between individuals and determine heirship and beneficiary status.
- Financial and Trust Asset Information – Includes information associated with Individual Indian Money (IIM) accounts and trust assets and is used to support the administration and distribution of estate assets.
- Legal and Probate Documentation – Includes wills, affidavits, birth certificates, death certificates, and estate records, which may contain multiple PII elements necessary to verify identity, relationships, and entitlement.
- Geospatial or Land Ownership Information – Includes data associated with trust land and asset locations that may be linked to individuals through ownership or probate case records and is used to support visualization and management of trust assets.
- User Account Identifiers – Includes usernames, system identifiers, and associated credentials for federal employees, contractors, and authorized users and is used for authentication, access control, and audit logging.
- Social Security Number (SSN) – May be collected where legally required for identity verification, estate claim validation, or financial account distribution, consistent with applicable federal requirements.

PII is collected directly from individuals submitting information through ENT, as well as from existing DOI systems used to support probate processing. The system limits collection to the minimum information necessary to support probate case processing and trust asset administration, and all PII is protected in accordance with applicable federal privacy and security requirements.

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

☒ Individual
☒ Federal Agency
☒ Tribal Agency
☐ Local Agency
☒ DOI Records
☒ Third Party Records
☒ State Agency
☐ Other: *Describe Below*

PII is collected directly from individuals, including decedents' families, heirs, beneficiaries, and authorized tribal representatives, through secure electronic submission within ENT using standardized forms and supporting documentation. PII is also obtained from DOI records, including BIA probate files, BTFA trust account systems, and LTRO land title data, to support case validation, asset identification, and probate processing. Additional PII may be obtained from federal, tribal, and state agencies, including vital records offices, as well as from third-party records such as historical probate files and documentation submitted by authorized representatives. Information is reviewed and cross-referenced, as appropriate, to ensure accuracy and completeness. ENT does not collect PII from local agencies or commercial data brokers.

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

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Website
☒ Fax
☒ Telephone Interview
☒ Shared Between Systems: *Describe*
☒ Other: *Describe*

The eNativeTrust System (ENT) collects PII through the following methods:

- **Website** – PII is collected through secure web-based forms, mobile submissions, and document uploads within the ENT portal, including digitized records from enterprise records management (ERM) systems. Data transmitted through the web interface is protected using HTTPS with Transport Layer Security (TLS) encryption.
- **Information Shared Between Systems** – PII is collected through automated data ingestion from Bureau of Indian Affairs (BIA) legacy probate systems and through secure system-to-system data exchanges with the Bureau of Trust Funds Administration (BTFA), Land Titles and Records Office (LTRO), and Office of Hearings and Appeals (OHA). Data is exchanged using encrypted connections within a FedRAMP authorized cloud environment.
- **Secure Document Upload and Automated Data Ingestion** – ENT supports secure upload of supporting documentation and automated processing of submitted records, including extraction and ingestion of relevant data elements. All automated processing is subject to human review and does not independently modify official records.

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

The eNativeTrust System (ENT) collects and uses PII to support probate case processing, trust asset administration, and coordination among authorized DOI offices and partners.

- **Heirship Verification and Family Relationship Determination** – PII is used to verify heirship, establish family relationships, and confirm identity of decedents, heirs, beneficiaries, and authorized representatives in support of probate case development.
- **Eligibility Validation and Case Adjudication** – PII is used to validate eligibility for inheritance, support adjudication of probate cases, and ensure that determinations are made in accordance with applicable

legal authorities and probate procedures.

- **Trust Asset Administration and Disbursement** – Financial and trust-related PII is used to process trust fund disbursements, including activities associated with Individual Indian Money (IIM) accounts and distribution of estate assets.
- **Probate Order Generation and Record Updates** – PII is used to generate probate orders and update land title ownership records, ensuring that official records accurately reflect adjudicated outcomes.
  Interagency Coordination and Data Exchange – PII is transmitted between Bureau of Indian Affairs(BIA), Office of Hearings and Appeals (OHA), Land Titles and Records Office (LTRO), and Bureau of Trust Funds Administration (BTFA) to support legally required actions, case processing, and record synchronization.

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

The eNativeTrust System (ENT) follows DOI's data minimization principle by collecting only the PII required to prepare probate files, verify identity, and process trust asset distributions.

- **Purpose-Based Collection** – PII collection is limited to the minimum necessary to prepare probate files, verify identity, and process trust asset distributions.
- **Limitation of Sensitive Data** – Sensitive identifiers, such as Social Security numbers (SSNs), are stored in restricted vault tables with masking to limit exposure.
- **AI Data Use Restrictions** – AI features are prohibited from training on production PII and instead use synthetic or de-identified data. AI-assisted functionality processes data within the system environment but does not retain, reuse, or train on production PII.
  Cloud Data Containment – AI large language models are maintained within the Azure FedRAMP environment to prevent information leakage outside of the authorized cloud environment.

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.

The eNativeTrust System (ENT) shares PII only with authorized recipients to support probate verification, cross-agency documentation, and required probate processing activities.

- **Within the Bureau/Office (Bureau of Indian Affairs)** – PII is shared with authorized BIA personnel to support probate verification, case processing, and documentation requirements.
- **Other DOI Bureaus/Offices** – PII is shared with other DOI offices involved in probate processing to support cross-agency documentation and coordination required for case adjudication.
- **Contractors** – PII may be shared with contracted support providers as necessary to perform system support, processing, and documentation functions. Contractor's access is limited to the information required to perform assigned duties.

- **Other Federal Agencies** – PII may be shared with other federal agencies pursuant to the routine uses described in the applicable System of Records Notice (SORN). Furthermore, it may be shared with state and local governments, or authorized third parties, as permitted by federal statute, regulations, or formal agreements.to support the various federal and tribal member or family probate verification and cross-agencies internal and external as other state and local government need.
- **Tribal, State, or Local Agencies** – PII may be shared with tribal governments and state vital records offices to verify identity, confirm documentation, and support probate case processing.
- **Other Third-Party Sources** – PII may be shared with authorized representatives acting on behalf of individuals to support probate verification and documentation submission.

All sharing is governed by written agreements requiring encryption, limited purpose use, and incident reporting. Data is transmitted using secure methods and is limited to the minimum necessary to support authorized functions.

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

The eNativeTrust System (ENT) shares PII under Memoranda of Understanding (MOUs), Interconnection Security Agreements (ISAs), or other inter-agency approvals, as applicable, for exchanges involving tribal enrollment data, land title information, state death records, and trust account data. These agreements reflect DOI privacy, security, and trust statutes.

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.*

Submission of probate documentation is required for case processing and cannot be declined without preventing case adjudication. The collection of PII is necessary to prepare probate files, verify identity, establish heirship, and process trust asset distributions. Individuals are informed of how their information is used through Privacy Act Statements and system notices provided at the point of collection. These notices describe the authority for collection, the purpose of the system, routine uses of the information, and the consequences of not providing the requested data. Optional data fields are minimized, and individuals may choose whether to provide any non-required information; however, required PII must be provided to proceed with probate processing.

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

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

The eNativeTrust System (ENT) informs people before collecting personal information by displaying Privacy Act Statements and layered privacy notices on public portal screens. It also provides internal notices for federal users. These notices describe the authority for collection, the purpose of the system, routine uses of the information, and the consequences of not providing the requested information.

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

ENT records are retrieved using identifiers specific to the individual or case, including name, case number, tribal enrollment number, address, date of birth, date of death, and other authorized case-related identifiers. Retrieval is role-based and limited to authorized personnel with a need to know.

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

ENT may generate individual-level probate case reports, document status reports, completeness reports, and case-processing reports containing PII to support probate case preparation, adjudication support, title updates, trust asset processing, and audit/accountability functions. Access to these reports is limited to authorized personnel, including assigned probate staff, the Office of Hearings and Appeals, Land Titles and Records Office, Bureau of Trust Funds Administration personnel, and other authorized users with a need to know. Reports are used only for official probate and trust administration purposes and are protected through role-based access controls, audit logging, and applicable Privacy Act and security safeguards.

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

The eNativeTrust System (ENT) receives PII from individuals, authorized representatives, tribal governments, state vital records offices, and other federal partners. Verification processes include:

- **Automated Field Validation** – The ENT web portal applies format and completeness checks at submission.
- **Cross-Referencing with Authoritative Sources** – Information is compared against existing DOI systems and records to confirm identity, relationships, and asset information.
- **AI-Assisted Review** – AI-assisted functionality may be used to identify required information and flag potential inconsistencies; all outputs are advisory and subject to human review.
- **Manual Review** – Probate personnel review documentation to identify discrepancies or missing information.
- **User and Source Confirmation** – Individuals or originating sources may be contacted to verify or correct information.
- **Error Correction** – Discrepancies are resolved prior to final case processing.

These processes ensure that PII is accurate, relevant, timely, and complete.

Section 4: Data Management and Retention

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

The eNativeTrust System (ENT) retains data in accordance with the following NARA-approved records schedules:

- **Probate Records** – Retained permanently in accordance with DOI and NARA trust and probate records schedule TR-46-31 governing Bureau of Indian Affairs probate records. ENT retains probate case files, supporting documentation, and decision records due to long-term trust obligations and their legal and historical significance. Permanent records are preserved and transferred to the National Archives and Records Administration (NARA) in accordance with approved schedules.
- **Digitized Records** – Retained permanently in accordance with the same applicable DOI and NARA-approved records schedules and integrated with the Office of Trust Records (OTR) Records Management Module (RMM) to ensure alignment with retention and records management requirements.
- **System-Generated Records** – Retained in accordance with GRS 3.2, Information Systems Security Records, which generally requires retention for one to several years depending on the record type. These records are temporary and are destroyed after the approved retention period in accordance with federal records management requirements.
- **Disposition of Electronic Records** – Electronic records are disposed of using secure methods in accordance with NIST SP 800-88 for media sanitization.

If new data elements or categories are introduced that are not covered under existing schedules, ENT will coordinate with the Bureau Records Officer to develop and obtain NARA approval for an appropriate records schedule prior to collection.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

The eNativeTrust System (ENT) applies multiple measures to validate the accuracy and completeness of PII received from external sources, including individuals submitting probate documentation, authorized representatives, tribal governments, and federal partners.

- **Cross-Referencing with Authoritative Records** – PII is cross-checked against federal and tribal records, as well as historical probate files, to confirm identity, relationships, and case information.
- **Required Documentation** – Individuals are required to submit supporting documentation, such as probate records and legal documents, to validate the accuracy of information provided.
- **Automated Data Validation** – Data is subject to automated validation and cleansing processes during ETL to identify inconsistencies and improve data quality.
- **Manual Review** – Authorized personnel review case files during case preparation and Office of Hearings and Appeals (OHA) proceedings to ensure completeness and accuracy.

These measures ensure that PII is accurate, relevant, timely, and complete, consistent with Privacy Act requirements.

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

☒ Yes
☐ No

The eNativeTrust System (ENT) includes logging capabilities to record and monitor access to PII.

- **Types of Logs** – ENT logs authentication events, including successful and failed login attempts, as well as PII access, downloads, edits, data transfers, and administrative actions.
- **Security of Logs** – Logs are maintained within DOI's enterprise monitoring environment and are protected through access controls to prevent unauthorized modification or deletion.
- **Retention** – Logs are retained in accordance with applicable DOI and NARA-approved records schedules, including General Records Schedule (GRS) 3.2, Information Systems Security Records, and are securely disposed of after the approved retention period.
- **Review Process** – Logs are integrated into DOI's enterprise monitoring capabilities for continuous monitoring, automated alerting, and incident investigation. Authorized personnel review logs as part of ongoing security operations and in response to suspected security or privacy incidents.

These measures support DOI's ability to detect, investigate, and respond to potential unauthorized access or misuse of PII.

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?

The eNativeTrust System (ENT) processes sensitive personal and tribal data, handles legal documentation, and integrates with multiple DOI systems, creating risks of unauthorized disclosure, data mismatches, role mis-assignment, over-collection, AI misinterpretation, and exposure of trust beneficiaries' information. ENT mitigates these risks through layered administrative, technical, and operational controls.

Collection:

- **Risks** – Risks include over-collection of PII, submission of inaccurate data, or collection without sufficient notice.
- **Mitigation:** PII collection is limited to the minimum necessary to process probate cases and validate identity and relationships. Required documentation supports data accuracy, and Privacy Act Statements inform individuals of the purpose and use of their information. Data is collected through secure, encrypted channels.

Use:

- **Risks** – Risks include unauthorized access, role mis-assignment, misuse of PII, and AI misinterpretation of legal documents.
- **Mitigation:** ENT enforces least privilege, role-based access controls and implements full audit logging of system activity. Sensitive data, such as Social Security numbers, is protected through PII vaulting. AI-assisted functionality is subject to Human-in-the-Loop oversight and is not used to make final determinations. AI training in production PII is prohibited.

Retention:

- **Risks** – Risks include prolonged retention of sensitive PII and potential exposure over time.
- **Mitigation** – Records are retained in accordance with DOI and NARA-approved records schedules. Electronic records are secured using FedRAMP-authorized cloud controls and are disposed of using secure methods consistent with NIST SP 800-88 where applicable.

Disclosure:

- **Risks** – Risks include unauthorized sharing, over-disclosure, or exposure of PII across interconnected DOI systems and external partners.
- **Mitigation** – PII is shared only with authorized entities for probate processing purposes under strict data-sharing agreements. Data is encrypted in transit and at rest, and access and data transfers are logged and monitored through DOI's enterprise monitoring capabilities.

Residual:

- **Risks** – Residual risks include data mismatches from external sources and handling of PII by external partners after disclosure.
- **Mitigation** – Data is validated through cross-referencing with authoritative records, required documentation, and human review. External partners are required to adhere to applicable privacy and security requirements.

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

The eNativeTrust System (ENT) generates limited derived data, such as completeness indicators, document-validation status, and case preparation metadata, to support probate case processing and adjudication. Derived data is generated from validated source records and reviewed by authorized personnel for accuracy before use. It does not create new facts about individuals and is used only to support authorized probate functions. Safeguards include FedRAMP security controls, encrypted storage and transmission, least-privilege role-based access, PII vaulting for sensitive data, audit logging, and Human-in-the-Loop oversight for AI-assisted outputs. The use of production PII for AI training is prohibited.

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

☒ Yes: *Provide explanation below*
☐ No

The eNativeTrust System (ENT) generates certain derived data, such as completeness indicators, document-validation status, and case preparation metadata, which become part of the individual's case record because they directly support heirship verification and case adjudication. These elements do not create new facts about individuals but reflect processing results (e.g., checklist confirmations and missing-document flags) needed to prepare legally sufficient probate packets for Office of Hearings and Appeals (OHA) review. Derived data is based on validated source records and is reviewed by authorized personnel prior to inclusion in the record.

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

☐ Yes: *Provide explanation below*
☒ No

The eNativeTrust System (ENT) does not make independent determinations about individuals based on derived data. Derived elements, such as completeness indicators and document-validation status, are used only to support case preparation and review. All determinations related to heirship and probate adjudication are based on verified source documentation and are made by authorized probate personnel, including review by the Office of Hearings and Appeals (OHA). The system does not perform automated decision-making, scoring, or predictive analysis that would result in determinations about individuals beyond what is supported by the original records.

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

The eNativeTrust System (ENT) verifies the relevance and accuracy of derived data through a combination of AI-assisted processing and human review.

- **Relevance Review** – Derived data, including outputs from AI-assisted tools such as OCR-based document classification, checklist validation, duplicate detection, and triage suggestions, is limited to supporting probate case preparation and remains consistent with the system's mission and purpose.
- **Accuracy Checks** – AI-assisted outputs are advisory only and are not used independently. All outputs are validated against source documentation and must be reviewed by authorized probate personnel before being used or incorporated into the case record.
- **Safeguards and Review** – AI is not used to adjudicate cases and may only operate on synthetic, masked, or de-identified data. Human-in-the-Loop oversight ensures that all derived data is accurate, relevant, and appropriate for its intended use.

These measures ensure that derived data is verified for accuracy and relevance prior to use in probate processing.

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?

ENT includes optional AI-assisted tools that perform document classification, detect missing evidence, and generate completeness indicators; these outputs are advisory only, require human review, and do not determine probate outcomes.

- **Accuracy (Validation & Testing)** – Outputs are validated against source documentation and case requirements, with human review prior to use. This supports ongoing evaluation of model performance and error detection.

- **Fairness (Bias Risk Management)** – AI functionality is limited to document processing and does not perform profiling, scoring, or predictive analytics. Human-in-the-Loop oversight mitigates the risk of biased or inappropriate outcomes.
- **Transparency (Explainability & Traceability)** – Outputs are explainable and traceable to underlying source records, enabling users to understand and verify how results were generated. System functionality and output are documented and auditable.

These controls align with federal AI governance practices, ensuring that AI-assisted capabilities remain accountable, reliable, and non-decisional.

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

☐ Yes
☒ No

ENT does not use AI to make or finalize decisions affecting an individual's rights, benefits, or participation. AI functionality is limited to advisory support activities, such as document classification, completeness review, and identification of potentially missing information, and all outputs are reviewed and validated by authorized personnel prior to use in case processing or entry into the official record. As a result, the system does not require a separate notice for AI-based decision-making; however, to support transparency, ENT provides layered privacy notices and contextual indicators within the system interface to inform users when AI-assisted tools are used.

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

☒ Yes
☐ No

The eNativeTrust System (ENT) applies safeguards to prevent bias and unintended consequences associated with AI-assisted functionality.

- **Human Oversight (HITL)** – All AI outputs are subject to required Human-in-the-Loop review and must be validated by authorized probate personnel prior to use. AI operates in a bounded, non-decisional role and cannot make autonomous determinations.
- **Data Controls and Testing Practices** – AI-assisted capabilities use synthetic, masked, or de-identified data during testing, reducing the risk of bias propagation and inappropriate exposure of sensitive information.
- **Monitoring and Operational Review** – AI outputs are reviewed during case preparation and adjudication processes to ensure they are applied appropriately and do not improperly influence outcomes. Audit logging and user oversight support detection of inconsistencies or unintended impacts.
- **Governance and Continuous Oversight** – Probate subject-matter experts provide ongoing oversight to validate output accuracy and ensure alignment with case requirements. Any identified issues are addressed through manual correction and process controls, rather than automated model adjustments.

These safeguards minimize the risk of algorithmic bias and unintended impacts while maintaining alignment with federal AI risk management principles, including human oversight, accountability, and controlled, non-decisional use.

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

☒ Yes
☐ No

AI-assisted features in the eNativeTrust System (ENT) undergo periodic evaluation during development sprints and system maintenance cycles to ensure ongoing reliability. Evaluations include documented testing, accuracy checks against source documentation, and peer review by probate subject-matter experts. Performance issues, including misclassifications or inconsistencies, are identified through operational use and Human-in-the-Loop review, and are addressed through refinement of AI logic, rule sets, or supporting checklists.

Where model updates or retraining are applicable, they are performed using synthetic, masked, or de-identified data, ensuring that production PII is not used. All AI outputs remain advisory and are subject to Human-in-the-Loop oversight. These practices support continuous improvement while maintaining alignment with the system's non-decisional design and established privacy and AI governance controls.

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

☐ Yes
☒ No

ENT does not use federated learning because AI functionality is strictly limited to advisory document-assistance features. No model training occurs on distributed user devices or decentralized data sources. All AI processing is conducted within a centralized, controlled environment supported by FedRAMP-Moderate security controls, and the use of live probate PII for model training is prohibited.

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

Access to eNativeTrust System (ENT) data is restricted based on role, bureau, and functional responsibility, and is granted strictly on a need-to-know basis. Access is enforced through Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and privileged access controls within a Zero Trust security architecture.

- **Users (Authorized Probate Personnel)** – Have read and/or edit access to probate case records as required to perform official duties such as case review, heirship verification, and document processing. Access is limited to assigned cases or jurisdictions.
- **System Administrators** – Have full administrative access to manage system configuration, user accounts, security settings, and monitoring functions. Access is restricted to privileged accounts and limited to authorized personnel performing system administration duties.
- **Contractors** – Have least-privilege, role-specific access limited to system maintenance, support, or operational tasks as defined in contract requirements. Contractor access is time-bound, monitored, and

subject to DOI security and privacy policies.

- **Developers** – Have limited access to development and testing environments only. Developers do not have access to production PII unless explicitly authorized, approved, and logged under controlled conditions.

Authorization and Access Controls – Access is provisioned through formal DOI access request workflows and requires System Owner approval based on role assignment and need-to-know determinations. The Information System Security Officer (ISSO) provides oversight for compliance with federal security requirements. All users must complete background screening (as applicable), accept DOI Rules of Behavior, and complete required security training prior to access approval.

Access is continuously enforced through MFA, RBAC, and privileged access controls. Accounts and permissions are periodically reviewed, and access is promptly revoked or modified upon role change or separation.

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

ENT operates entirely within the BIA eNativeTrust Microsoft Azure Government tenant in a FedRAMP-Authorized Moderate cloud environment.

Cloud-based PII storage complies with:

- **DOI Cloud Computing Policy** – Requires use of FedRAMP-authorized cloud services for systems processing PII.
- **FedRAMP Moderate Baseline (NIST SP 800-53 Rev. 5)** – Establishes required controls for access management, audit logging, incident response, system integrity, and contingency planning.
- **NIST SP 800-144 (Cloud Computing Security Guidance)** – Provides guidance for cloud security architecture, shared responsibility, and risk management.

ENT implements layered security architecture including Zero Trust principles, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Web Application Firewall (WAF) protection, API Management (APIM)-secured interfaces, and Microsoft Sentinel SIEM for FISMA-aligned continuous monitoring. All PII is protected using FIPS 140-2 validated encryption at rest and in transit. Access is restricted under least-privilege principles and continuously monitored through centralized logging and alerting.

The system performs daily incremental and weekly full backups for all system and user-level data. Azure Geo-Redundant Storage (GRS) provides physical and logical separation from the primary environment to ensure resilience and availability. Backup integrity is verified using cryptographic hashing and digital signatures to detect unauthorized modification. Quarterly restoration testing ensures Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are met in accordance with the Information System Contingency Plan (ISCP). All controls are continuously monitored to ensure compliance with DOI and federal requirements for safeguarding PII in cloud environments.

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

The eNativeTrust uses multiple integrated monitoring capabilities to detect and respond to unauthorized access, use, or potential security incidents involving PII.

- **Automated Monitoring Tools** – Microsoft Sentinel Security Information and Event Management (SIEM) is used to aggregate system logs from Azure Monitor, Log Analytics, Azure Activity Logs, API

Management (APIM), and Entra ID. These logs are analyzed to identify and generate alerts for unusual or potentially suspicious system activity.

- **Access Audit Logs** – ENT records all PII access events, including user identity, timestamp, and activity type. These logs are centrally stored and used for monitoring, auditing, and incident investigation.
- **Alert Response Process** – Alerts generated by the SIEM platform are routed to designated security personnel, including the Information System Security Officer (ISSO), for review and investigation. Alerts are analyzed and escalated in accordance with DOI incident response procedures and applicable federal requirements, including NIST SP 800-53 Rev. 5 (AU, IR, and SI control families) and OMB M-07-16 breach notification guidance.

These monitoring and logging capabilities support detection, review, and response to potential unauthorized activity involving PII in accordance with federal privacy and security requirements.

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 eNativeTrust includes monitoring of user activity to protect system security, maintain data integrity, and support federal audit and accountability requirements.

Monitored Activities

- Login attempts (successful and failed)
- Data access events involving PII and case records
- Record creation, modification, and system interaction activities
- Administrative and privileged account actions
- API activity through API Management (APIM)-secured endpoints

Controls for Appropriate Use

- Monitoring data is accessible only to authorized personnel, including Information System Security Officers (ISSO), system administrators, and designated security personnel with a documented need-to-know.
- All monitoring activities are logged and subject to review as part of continuous monitoring and incident response procedures.
- DOI Rules of Behavior and required security and privacy training inform users that system activity is monitored and establish acceptable use expectations.
- Any use of monitoring data for investigation purposes follows DOI incident response procedures and is documented for accountability and oversight.

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

☒ Design
☒ Development

☒ Maintenance

Contractors are involved in the following eNativeTrust System (ENT) project activities:

- **Design** – Contractors support system design activities, including workflow configuration and interface design for probate case management functions.
- **Development** – Contractors develop and configure system functionality, including application updates and secure API integrations within the Azure Government environment.
- **Maintenance** – Contractors provide ongoing system maintenance, including patch management, troubleshooting, and system performance monitoring.

Some contractor personnel may have limited access to PII when required for system development, testing, troubleshooting, or maintenance activities. Access is granted on a least privilege, need-to-know basis and restricted to authorized roles. All contractor personnel with access to ENT data are required to:

- Sign non-disclosure agreements (NDAs)
- Comply with applicable Federal Acquisition Regulation (FAR) Privacy Act clauses (including FAR 52.224-1 and 52.224-2)
- Complete DOI-approved annual privacy and security training
- Adhere to DOI Rules of Behavior and system access procedures

Contractor access is provisioned based on role and is subject to periodic review by the System Owner and Information System Security Officer (ISSO).

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

Physical Controls

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☐ Identification Badges
☐ Safes
☐ Combination Lock
☒ Other: *Describe Below*

Physical safeguards for ENT are provided primarily through the Azure Government hosting environment operating under FedRAMP-authorized controls, including facility access restrictions, environmental protections, hardware inventory protections, and monitored data center operations. Any DOI-managed administrative access points or supporting facilities are also subject to DOI physical access controls and facility security requirements.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Biometrics

Administrative Controls

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

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

Individuals may file a Privacy Act complaint regarding the eNativeTrust System (ENT) through the Department of the Interior's established Privacy Act complaint process:

- **Submission Methods** – Complaints may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or through the DOI FOIA/Privacy Act request portal.
- **Responsible Office** – The DOI Chief Privacy Officer receives Privacy Act complaints and assigns them to the appropriate Privacy Officer or Privacy Analyst for review and coordination.
- **Review Process** – The assigned reviewer evaluates the complaint, coordinates with the System Owner and relevant program staff, and determines whether a Privacy Act issue or violation has occurred.
- **Resolution and Response** – DOI provides a written response to the complainant outlining the findings and any corrective actions taken in accordance with DOI privacy procedures.
- **Notice to Individuals** – Individuals are informed of their rights to file a complaint through Privacy Act Statements on system collection points and applicable System of Records Notices (SORN).

This process is conducted in accordance with **43 CFR Part 2, Subpart K**, which establishes DOI's procedures for handling Privacy Act complaints.

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

Individuals may access their records in the eNativeTrust System (ENT) by submitting a Privacy Act request through the Department of the Interior's established process.

- **Request Methods** – Requests may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240 or through the DOI FOIA/Privacy Act request portal. Requests must include the individual's full name, contact information, a description of the records sought, and proof of identity (e.g., a signed statement or declaration under penalty of perjury).
- **Responsible Office** – The DOI Departmental Privacy Office, in coordination with the appropriate Bureau Privacy Officer, is responsible for receiving and processing Privacy Act access requests.
- **Processing and Review** – Upon receipt, the Privacy Office verifies the identity of the requester, confirms whether ENT contains records about the individual, and coordinates with the System Owner and program staff to locate responsive records.
- **Response** – DOI responds to requests within the timeframes established in 43 CFR Part 2, Subpart K, providing access to records or explaining any applicable exemptions or redactions.

- **Notice to Individuals** – Information on how to request access to records is provided in applicable System of Records Notices (SORN) and Privacy Act Statements presented at system collection points.

This process is conducted in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K, ensuring individuals can access their records while protecting the security and integrity of the information.

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

Individuals may request correction of inaccurate or erroneous information maintained in the eNativeTrust System (ENT) in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests for amendment may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, or through the DOI FOIA/Privacy Act request portal. Requests must include sufficient identifying information, a description of the information to be corrected, and verification of identity.
- **Processing and Review** – Upon receipt, the DOI Privacy Office reviews the request for completeness and verifies the identity of the requester. The Privacy Office coordinates with the ENT System Owner and relevant program staff to evaluate the accuracy of the information and determine whether an amendment is appropriate.
- **Response** – DOI responds in accordance with applicable regulations, either making the requested correction or providing a written explanation if the request is denied, including information on how to appeal the decision.
- **Limitations** – Because ENT maintains official probate case records, amendments are limited to correcting inaccurate or erroneous information. Records required to preserve the integrity of official case files may not be altered; however, supplemental or clarifying information may be added to the record where appropriate.

This process ensures compliance with Privacy Act amendment provisions while maintaining the integrity and legal sufficiency of official probate records.

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 Information System Owner is responsible for ensuring ENT data is used only for authorized probate and trust administration purposes and that access is limited based on role and need to know. The Information System Security Officer (ISSO) is responsible for monitoring compliance with system security controls, audit logging, and incident response coordination. Users, administrators, and contractors with access to ENT data are responsible for complying with DOI Rules of Behavior, annual privacy and security training, and prompt reporting of any suspected or confirmed loss, compromise, unauthorized disclosure, or unauthorized access involving privacy-protected information. Suspected or confirmed incidents must be reported within one hour to DOI-CIRC and the DOI Privacy Office in accordance with DOI policy and the DOI Privacy Breach Response Plan.

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 privacy breach involving the eNativeTrust or the eNativeTrust System (ENT), the Department of the Interior will follow the procedures outlined in the DOI Privacy Breach Response Plan:

1. **Immediate Reporting** – Any suspected or confirmed breach must be reported within one hour of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. **Containment and Mitigation** – The Information System Security Officer (ISSO), System Owner, and DOI-CIRC work to secure affected systems, revoke compromised credentials, and prevent further unauthorized access or data loss.
3. **Risk Assessment** – The Privacy Officer and breach response team assess the nature and scope of the incident, including the type of PII involved, the number of individuals affected, and the potential risk of harm.
4. **Notification** – When required, affected individuals will be notified without unreasonable delay, consistent with OMB guidance and DOI policy. Notifications include a description of the incident, the types of information involved, individuals can take to protect themselves and contact information for assistance.
5. **Oversight Reporting** – DOI will report incidents to oversight bodies, including OMB, Congress, and the Department of Homeland Security (DHS), when thresholds for major incidents are met.
6. **Remediation and Prevention** – The system team will implement corrective actions, such as enhancing security controls, updating procedures, and retraining personnel to reduce the likelihood of recurrence.

These standards guarantee a coordinated, prompt, and compliant approach to reducing harm to individuals and safeguarding their well-being.
the integrity of ENT data.

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

This PIA will be reviewed at least annually as part of DOI system oversight, FISMA reporting, BisonGRC updates, system reauthorization, or other periodic review processes, and it will be updated whenever significant changes occur to the ENT environment, including technology changes, data practices, provider relationships, approved service capabilities, AI capability changes, user populations, or privacy risk posture.