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:	Federal Acknowledgment Information Resource
System or Project Acronym:	FAIR
Date submitted for review:	May 14, 2026
System Operational Status:	Development

Point of Contact

Name:	Nikki Bass
Title:	Director
Office:	Office of Federal Acknowledgment
Phone:	202-513-7650
E-mail:	Nikki.Bass@indianaffairs.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

This PIA is being updated to reflect significant system enhancements, including the implementation of a user portal that will provide petitioners and authorized users with a centralized interface to submit, access, and manage petition-related information. This is an update to the PIA published in 2025.

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

The new FAIR is a cloud-based and cloud-hosted application designed to support The Office of Federal Acknowledgment's (OFA) activities, including the review and maintenance of petition submissions for Federal Acknowledgement of American Indian Tribes. The Office of Federal Acknowledgment (OFA) within the Office of the Assistant Secretary - Indian Affairs (AS-IA) of the Department of the Interior (Department) implements the requirements of 25 CFR Part 83, Federal Acknowledgment of American Indian Tribes. The acknowledgment

process is the Department's administrative process by which petitioning groups that meet the criteria are given federal "acknowledgment" as Indian Tribes and by which they become eligible to receive services provided to members of Indian Tribes. As a result, the creation of the Federal Acknowledgment Information Resource (FAIR) system, a cloud-based, Department of the Interior (DOI) information system operated by the Bureau of Indian Affairs (BIA), Office of Federal Acknowledgment (OFA), addresses the requirements. The system is designed to support the administrative process for evaluating petitions submitted by groups seeking federal acknowledgment as American Indian Tribes in accordance with 25 CFR Part 83.

FAIR provides a centralized, secure platform for the collection, storage, management, and analysis of petition-related information and supporting documentation. The system enables authorized internal users, including federal employees and contractors, to review, process, and evaluate petition submissions using established anthropological, genealogical, and historical research methodologies. FAIR includes an external, web-based submission portal that allows authorized external users—such as petitioning groups, federally recognized Tribal governments, State and local governments, and members of the public—to electronically submit petitions (to be federally recognized as members of an Indian Tribe), supporting documentation, comments, and inquiries. This functionality enhances transparency, improves processing efficiency, and reduces reliance on manual or paper-based processes. The system supports the full lifecycle of the acknowledgment process, from initial submission through final determination.

The system collects and maintains personally identifiable information (PII) and sensitive data necessary to support the acknowledgment process, including but not limited to identifying information, genealogical records, and historical documentation. FAIR implements administrative, technical, and physical security controls in accordance with federal requirements, including the Federal Information Security Modernization Act (FISMA), the Privacy Act of 1974, and applicable National Institute of Standards and Technology (NIST) standards, to safeguard information and mitigate privacy risks. FAIR operates within a DOI-approved cloud environment and leverages enterprise authentication services, including Login.gov for external to DOI users, to ensure secure user access through multi-factor authentication. Access to system data is role-based and restricted to authorized users with a demonstrated need-to-know, consistent with the principle of least privilege.

FAIR supports the Department's mission to ensure a consistent, transparent, and efficient process for determining federal acknowledgment eligibility while maintaining the confidentiality, integrity, and availability of sensitive information.

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.

UII Code: 010-000000018, Federal Acknowledgement Information Resource System (FAIR)

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

The collection, maintenance, and use of information within this system are authorized by the following statutes and regulations:

- **25 CFR Part 83** – Federal Acknowledgment of American Indian Tribes
- **25 U.S.C. §§ 2 and 9** – Duties of the Commissioner of Indian Affairs
- **Pub. L. 103-454, 108 Stat. 4791** – Federally Recognized Indian Tribe List Act of 1994

- **43 U.S.C. § 1457** – Department of the Interior and Related Agencies Appropriations Act
- **5 U.S.C. § 301** – Government Organization and Employees

These authorities authorize the Department to receive, review, evaluate, and maintain petition documentation and records associated with acknowledgment determinations.

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

Yes. During the development of this PIA, the OFA identified the need to publish a new SORN to cover FAIR records, which has been drafted by the program office with the assistance of the IA Associate Privacy Officer (APO) and will be submitted to the Federal Register for publishing. This PIA will be updated after the new SORN is published in the Federal Register. The system requires a Privacy Act Statement at the point of collection because it includes a public-facing portal that collects personally identifiable information (PII) directly from individuals and petitioning entities. The FAIR portal includes a Privacy Act Statement/Privacy Notice on data collection interfaces, such as the document upload ("My Documents") page, to inform users about the authority for collection, the purpose of the collection, how the information will be used, whether submission is voluntary or required, and the consequences of not providing the requested information.

Employee user credential records are covered under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), modification published at 86 FR 50156 (September 7, 2021). GSA maintains records on individuals who use Login.gov and has published a SORN for the system: GSA/TTS-1 (Login.gov) - 87 FR 70819 (November 21, 2022). The SORN is available for review on the GSA SORNs web page.

In the interim, the system provides clear and comprehensive notice to individuals at the point of collection to ensure transparency and compliance with the Privacy Act of 1974 and applicable federal guidance.

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

☒ Yes
☐ No

Yes. The system involves information collections that are subject to approval under the Paperwork Reduction Act (PRA). The FAIR system supports the collection of information associated with the federal acknowledgment process, which is covered under an approved Office of Management and Budget (OMB) Control Number.

Specifically, OMB Control Number 1076-0104, "Federal Acknowledgment as an Indian Tribe (25 CFR Part 83)," expiration date of December 31, 2028, applies to the collection of petition materials submitted through the system, including required forms such as the Individual History Chart (BIA-8304), Ancestry Chart (BIA-8305), and Membership List (BIA-8306).

Providing this information is necessary for the Department to evaluate petitions for federal acknowledgment.

Therefore, the system operates in compliance with PRA requirements, and all applicable collections are covered under the existing OMB approval.

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

The FAIR system does not include any minor applications or subsystems

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 or 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
☒ Tribal or other ID number	☐ Education information	☐ Disability Information
☐ Military records	☒ Other: Describe below	

Because 25 CFR Part 83 allows for a petitioner to submit a petition in "any readable form" (§ 83.21(a)) and third parties can submit whatever information they wish, there is considerable latitude across cases as to any additional information about individuals, living or dead, that would be incidentally collected and maintained in the system and properly safeguarded. Work related contact information such as name and password, work email, and work telephone number are collected from federal employees and contractors from users to create accounts to access the system.

In addition to the personally identifiable information (PII) identified above, petitioner documentation may include maiden name, records of birth, baptism, adoption, degree of Indian blood, Tribal/band affiliation, death certificate, name of petitioner's father and mother; name of petitioner's brothers and sisters; and name of individual preparing the BIA-8304, and Individual History Chart (if the person preparing is not a member of the group defined by 25 CFR 83.1).

Petition notification records may include:

- Names, addresses, telephone number, fax number, email address, and other publicly available information of the governor or attorney general of the State in which the petitioner is located; Government of the county-level (or equivalent) jurisdiction in which the petitioner is located;
- Any recognized Tribe and petitioner that appears to have a historical or present relationship with the petitioner or that may otherwise be considered to have a potential interest in the acknowledgment determination;

- Any comments or materials submitted by third parties to OFA relating to the documented petition;
- Any substantive letter, proposed finding, recommended decision, and final determination issued by the DOI;
- OFA's contact list for each petitioner, including the point of contact for the petitioner;
- Attorneys and representatives; and
- Contact information for any other individuals and entities that request to be kept informed of general actions regarding the petitioner.

The petition review record may include name, office address, work telephone number, and work email address of the OFA staff member with primary administrative responsibility for the petition; researchers conducting the evaluation of the petition; and the OFA staff member supervisor.

For a list of PII collected by Login.gov, see the GSA Login.gov PIA at Login_PIA_(March_2026).pdf.
For a list of PII collected through the use of PIV cards (government employees), see the DOI Enterprise Hosted Infrastructure (EHI) PIA at Enterprise Hosted Infrastructure (EHI) PIA.

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*

Another petitioner that appears to have a historical or present relationship with the petitioner or that may otherwise be considered to have a potential interest in the acknowledgment determination; individuals that request to be kept informed of general actions regarding the petitioner; attorneys and representatives; DOI employees and contractors with primary administrative responsibility for a petition; researchers conducting the evaluation of a petition; OMB approved Federal Acknowledgment as an Indian Tribe (OMB No. 1076-0104) information collection; corporations and other business entities, which are not subject to the Privacy Act; and individual members of the public who communicate, interact with, or request assistance or services from the DOI.

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

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

Information is collected through a secure web-based portal within the BIA OFA environment. External users authenticate via Login.gov and submit petitions, supporting documentation, comments, and related materials electronically. Submitted files are stored in a BIA-managed cloud storage environment. Each submission generates a document record within FAIR, and uploaded files are stored in a BIA-managed Azure Blob Storage container (FedRAMP-authorized). Metadata associated with submissions includes submitter identity, submission date, document descriptions, and related comments.

FAIR uses Login.gov only for external petitioners and authorized non-Federal users accessing the submission portal. Internal DOI users access FAIR through DOI network credentials covered under INTERIOR/DOI-47. These access paths are separate and governed by distinct credentialing requirements..

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

The PII collected in FAIR is used by the Office of Federal Acknowledgment (OFA) to support the evaluation of petitions for federal acknowledgment as American Indian Tribes under 25 CFR Part 83. The information is used to verify identity, lineage, and group membership through anthropological, genealogical, and historical analysis. It supports the review and validation of petition materials, facilitates communication with petitioners and authorized representatives, and enables the Department of the Interior to make informed decisions regarding eligibility for federal recognition. The information is also used to maintain official records, support administrative and legal processes, and fulfill the Department's responsibilities under applicable laws and regulations.

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

FAIR limits the collection and use of PII to only what is necessary to support the federal acknowledgment process under 25 CFR Part 83. FAIR does not require SSNs for petition review. SSNs may appear incidentally in petitioner-submitted documents. OFA instructs petitioners to avoid including SSNs where possible, consistent with DOI SSN Reduction Policy and OMB M-17-12. Any SSNs received are not used for identity verification and are redacted or sequestered when not essential for lineage validation.

Access to PII is restricted through role-based access controls and the principle of least privilege, ensuring that only authorized personnel with a need-to-know can view or use the information. The system enforces data minimization through administrative policies, user training, and technical controls that limit access, use, and sharing of information to official purposes only. Additionally, records are maintained and retained in accordance with approved records schedules, ensuring that information is not kept longer than necessary for operational and legal 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 the Bureau/Office: Information may be shared with BIA employees acting in their official capacity in the performance of official functions to comply with 25 CFR Part 83. The Assistant Secretary – Indian Affairs has access to the information to make final determination on a petition.

Other Bureaus/Offices: Office of the Solicitor and Office of Hearing and Appeals access the information to make

recommendations to the Assistant Secretary – Indian Affairs.

Other Federal Agencies: Under 25 CFR 83.22(b)(1), the OFA publishes notice in the Federal Register that a group has filed a documented petition for Federal acknowledgement as an American Indian Tribe to the Assistant Secretary Indian Affairs.

Contractor: Information may be shared with BIA contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support.

Other Third- Party Sources: Under 25 CFR 83.21(b) and 25 CFR 83.22(b)(1) petitioner's name and mailing address are made available to the public. Information may also be shared with another petitioner that appears to have a historical or present relationship with the petitioner or that may otherwise be considered to have a potential interest in the acknowledgment determination; individuals that request to be kept informed of general actions regarding the petitioner; attorneys and representatives; recognized Tribes and interested private parties; and State and local government officials, and federally recognized Tribes .

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

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.*

PII is provided primarily by petitioners who present their membership rolls and files for analysis in conjunction with 25 CFR Part 83 regulations. It is the petitioning entity that submits PII directly to OFA not individuals therefore, individuals cannot object or withhold their consent since it is the petitioning entity that submits the PII as part of their petition materials and in adherence to 25 CFR Part 83. By submitting a petition, they know their PII will be reviewed.

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.*

During the development of this PIA, the OFA identified the need to publish a new SORN to cover FAIR records, which has been drafted by the program office with the assistance of the IA Associate Privacy Officer (APO) and

will be submitted to the Federal Register for publishing. This PIA will be updated after the new SORN is published in the Federal Register.

For external DOI users such as the general public, notice is provided through publication of this PIA. Before using the Login.gov service, individuals must read and acknowledge that they accept the Login.gov Rules of Use published by GSA. If the Login.gov service changes its terms of service; users will be given the option to agree to or decline the updated terms of service, the next time they log in Login.gov provides a link to its Privacy & Security page on both the sign-in and create account pages. GSA has published GSA/TTS-1 (Login.gov), 87 FR 70819 (November 21, 2022). The SORN is available for review on the GSA SORNs web page complete with Privacy Act Statement and published Privacy Practices. Additionally the Login.gov PIA is available for review on the GSA PIA web page.

DOI 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.).

Records in FAIR are primarily retrieved by name, petitioner acronym, and petition number.

Note: As part of 25 CFR Part 83 acknowledgment process, a petitioner and other parties are entitled to submit documents that describe specific individuals. These individuals might be living or deceased, and the documents might date back to the 19th century. Such documents might be tagged with metadata that included the name of an individual, thus making the document retrievable by name.

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

While, audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system, it's used to track any user abnormalities from a systems-level (i.e. not directed to any particular user). Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit logs also collect information on system users such as usernames. System administrators and the information system owner have access to these activity reports.

Login.gov may produce compliance/audit reports on individuals' actions in the system for investigatory and fraud mitigation purposes. FAIR users may review the GSA Login.gov PIA for information on reporting functions within the system and how GSA generates, uses, and shares reports on individuals.

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

Login.gov ensures the accuracy and completeness of the user's email address and multi-factor authentication

(MFA) method by requiring the user to confirm their email address and utilize an acceptable MFA method. FAIR users may review the GSA Login.gov PIA for information on how GSA will check their PII for accuracy when logging into the system.

If an individual believes their records are not accurate, they can request corrections or the removal of material from the record by writing to the Indian Affairs (IA) APO. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K.

Section 4: Data Management and Retention

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

Records are covered by Indian Affairs Records Schedule (IARS) Records Series 3201-P5 – Acknowledgment Files and have been scheduled as permanent records under the National Archives and Records Administration (NARA) Job No. N1-075-05-001, approved March 31, 2005. Records may include documents associated with groups applying for federal recognition as an Indian Tribe. Files contain the letter of petition, responses to criteria for service eligibility (25 CFR § 83.11(a-g)), findings for/against acknowledgment of the group and final determination reports. Records are maintained in the office of records for a maximum of 5 years. Records are cut-off and the end of the fiscal year. The records are then retired to the American Indian Records Repository (AIRR), which is a Federal Records Center (FRC). Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the DOI and NARA.

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three years after cut-off.

GSA is responsible for managing its Login.gov records in accordance with the Federal Records Act and approved records retention schedules. The Login.gov PIA contains additional information about GSA's retention of Login.gov records.

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

It is the responsibility of the petitioner to ensure information provided in the forms and incidental records is accurate. Data is checked for accuracy during the account creation process. Users are responsible for ensuring the accuracy of the data associated with their user accounts.

OFA then verifies external genealogical, historical, and lineage records using cross-source validation including official vital records, census data, archival records, and documented Tribal materials. Records inconsistent with CFR Part 83 criteria are flagged for further review.

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

☒ Yes
☐ No

User actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Login.gov logs monitor user sign-in authentication actions. Users may review the Login.gov PIA for additional Information.

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?

There is a risk to the privacy of individuals due to the sensitive PII contained in FAIR. FAIR has undergone a formal Assessment and Authorization in accordance with the FISMA and NIST standards. FAIR is rated as a FISMA moderate system and requires administrative, physical, and technical controls established by NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. DOI requires multi-factor authentication (MFA) for network and system access. Only authorized personnel with proper credentials can access the records in the system. Access restrictions on data and various parts of the system's functionality are role-based and require supervisory approval. Access control lists were created and segmented, users cannot view information for other users unless specifically authorized. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. FAIR meets BIA's information system security requirements, including operational and risk management policies. Additionally, BIA manages user accounts using the Bison System Access Management (BSAM) system to manage access. BSAM is the DOI-wide authoritative source for all identities and the primary solution for Identity Lifecycle Management (ILM). BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards and until their departure from DOI. BSAM is used to establish, activate, modify, review, disable user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts at unauthorized access or scanning of the system are reported to IT Security.

There is a risk that FAIR may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained to provide a service or perform official functions. Authorized personnel with access to

the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions.

The BIA follows the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI network requires MFA authentication. Users are granted authorized access to perform their official duties, and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST SP 800-53. DOI employees must take Information Management and Technology (IMT) Awareness training which includes Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, Controlled Unclassified Information (CUI), Paperwork Reduction Act (PRA), and Forms Compliance before being granted access to DOI information and information systems, and annually thereafter. DOI personnel also sign the DOI Rules of Behavior. Personnel with significant privacy responsibilities must also take role-based privacy training annually to ensure an understanding of their responsibility to protect privacy. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

In terms of mitigating the risk of user error, DOI employees most complete annual privacy awareness training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they understand their responsibility to protect privacy. Users are advised not to share sensitive data with individuals without authorized access and to review the applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements.

There is risk of maintaining inaccurate information. This risk is mitigated by the following: (1) it is the responsibility of the petitioner to provide accurate and current information, and (2) once the petitioner submits their materials, OFA staff[1] checks for completeness to determine whether the submission complies with 25 CFR Part 83.21. Petitioner materials must meet all the requirements in Part 83.21 for their records to be ready for evaluation by OFA staff.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or

[1] Staff genealogists use a petitioner's membership files to review birth, death, and marriage certificates that might be contained in those files to trace family ancestry back to members of a historical Indian Tribe. The genealogists use Excel to create a spreadsheet showing the generation-to-generation genealogy of each member of the petitioning group. They use Ancestry.com to obtain census and other records that can help identify early ancestors. They may also examine public records such as annuity lists, treaties, claims rolls, or any other information that would identify a historical Indian tribe. Finally, they may use copies of family bibles provided by petitioners or oral histories to identify ancestors as well.

in accordance with an approved records retention schedule. The OFA is responsible for managing and disposing of BIA records in FAIR as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. OFA ensures only records needed to support its program, Tribes, and Tribal members are maintained. OFA maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the AIRR, an FRC, for permanent safekeeping in accordance with retention schedules approved by NARA under Job No. N1-075-05-001: 3201-P5, Acknowledgment Files. FAIR system usage records are covered by DRS 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut off when superseded or obsolete and destroyed no later than 3 years after they are cut off. Information collected and stored within FAIR is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. GSA is responsible for mitigating privacy risk by maintaining Login.gov records in accordance with NARA-approved records schedules.

There is a risk that data may not be securely stored in the service provider's system or that the vendor may not handle or store DOI PII according to DOI policy. FAIR operates within the Department of the Interior (DOI) Microsoft Dynamics 365 environment, a Software-as-a-Service (SaaS) platform deployed inside a Microsoft FedRAMP-authorized security boundary. FAIR holds a current agency Authorization to Operate (O-ATO) aligned with NIST Special Publication (SP) 800-53, Revision 5. The FAIR security package was developed and assessed by the DOI Center of Excellence—Information Management and Assurance Program Support (IMAPS) team. The combination of security controls provided by the Microsoft Dynamics 365 cloud service and bureau-implemented controls establishes an acceptable risk posture for a system categorized as *Moderate* impact under FIPS 199. For information uploaded by public users, data are stored within the Indian Affairs Azure Applications (IA-AA) authorization boundary where vulnerability scanning, and sensitive-information monitoring are conducted. Audit logs are maintained sufficiently to reconstruct security-relevant events.

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

FAIR is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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

☐ Yes: *Provide explanation below*
☒ No

FAIR is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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

☐ Yes: *Provide explanation below*

☒ No

FAIR is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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?

N/A

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

☐ Yes
☐ No

N/A

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

☐ Yes
☐ No

N/A

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

☐ Yes
☐ No

N/A

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

☐ Yes

☐ No

N/A

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*

Users are only given access to data based on the “least privilege” principle combined with a “need-to-know” to complete assigned duties. BIA manages user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for ILM. BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards and until their departure from DOI. BSAM is used to establish, activate, modify, review, disable user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for Tribal members working on a program, which must be approved by the program manager.
External FAIR user access is authenticated by Login.gov.

GSA Login.gov privileged users may have access to view data supplied by individuals to GSA for their user accounts and for identification verification and authentication but cannot amend or delete PII data within a record. GSA does not have access to any data stored in FAIR that is not publicly available.

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

FAIR operates within a DOI-approved cloud environment that complies with Federal Risk and Authorization Management Program (FedRAMP) requirements. The system implements security and privacy controls in accordance with NIST SP 800-53. Firewalls and network security configurations are also built into the architecture of the system. PII stored in the cloud is protected through administrative, technical, and physical safeguards, including encryption of data at rest and in transit, multi-factor authentication (MFA), role-based access controls, audit logging, and continuous monitoring. DOI ensures compliance with departmental policies, including DOI Cloud Computing Policy and information security standards. These controls collectively ensure the confidentiality, integrity, and availability of PII. All Login.gov traffic is subject to monitoring and recording to identify unauthorized attempts to change information or jeopardize the confidentiality, integrity, or availability of Login.gov.

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

FAIR can audit the usage activity within the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent

unauthorized monitoring. System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. System Administrators assign user roles based on the principle of 'least privilege' and perform due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to FAIR Rules of Behavior. Users must complete annual IMT Awareness training, which includes Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, CUI, Paperwork Reduction Act, and Forms Compliance before being granted access to DOI information and information systems, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The FAIR audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security.

Login.gov audits access, vets privileged users and enforces principles of least-privileged access to decrease the risk of abuse. For additional information about controls that GSA uses to prevent unauthorized monitoring, users may review the Login.gov PIA.

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

FAIR can audit the usage activity within the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring. System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. System Administrators assign user roles based on the principle of 'least privilege' and perform due diligence toward ensuring that separation of duties is in place.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The FAIR audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts at unauthorized access or scanning of the system are reported immediately to IT Security.

In addition, all users will be required to consent to FAIR Rules of Behavior. Users must complete annual IMT Awareness training, which includes Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, CUI, PRA, and Forms Compliance before being granted access to DOI information and information systems, and annually thereafter. Login.gov audits access, vets privileged users and enforces principles of least-privileged access to decrease the risk of abuse. For additional information about controls that GSA uses to prevent unauthorized monitoring, users may review the Login.gov PIA.

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

☒ Design
☒ Development
☒ Maintenance

Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The privacy terms and conditions and 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 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

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*

· Secured facility access using badge readers and on-site security guards.
· Locked filing cabinets within a locked room at MIB.
· Video surveillance (CCTV) covering all data center entry points.
· Other: Use of visitor logs and escorted access for all non-cleared personnel entering secured areas.

Technical Controls

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

· Multi-factor authentication (MFA) for all user accounts.
· Encryption of PII at rest using FIPS 140-3 validated algorithms and in transit via TLS 1.2 or higher.
· Role-based access controls (RBAC) restricting data access to authorized users with a demonstrated need-to-know.
· Firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and block unauthorized network

traffic.
· Other: Session timeout and automatic logoff after 15 minutes of inactivity to reduce the risk of unauthorized viewing on unattended devices.

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

· Annual DOI privacy and security training for all users, including contractors with PII access.

- Periodic security audits and vulnerability scans to assess control effectiveness.

· DOI Rules of Behavior acknowledgment required before account activation.

· Regular access reviews to ensure privileges remain appropriate for user roles.

· Other: Formal incident response procedures that require reporting suspected privacy breaches to the DOI-CIRC and Privacy Officer within one hour.

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

The Deputy Associate Chief Information Officer serves as the Information System Owner (ISO) for FAIR. The ISO, Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for oversight and management of security and privacy controls and the protection of IA information processed and stored by FAIR. The ISO is responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by Indian Affairs. The ISO is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the DOI OCIO Privacy Officer. All Privacy Act complaints will be processed through the Department OCIO office.

GSA is responsible for the management of Login.gov, meeting the requirements of the Privacy Act and other Federal regulations, and protecting individual privacy for the information collected, maintained, used, and transmitted by GSA for identity verification and authentication purposes.

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

Individuals may request access to their records under the Privacy Act of 1974 or the Freedom of Information Act

(FOIA), as applicable.

Requests for access must be submitted in writing and should include sufficient identifying information to locate the records. Requests are processed in accordance with DOI Privacy Act regulations (43 CFR Part 2, Subpart K) and FOIA requirements.

Individuals may submit requests to the DOI Privacy Office or the appropriate bureau office. Identity verification is required prior to releasing records to ensure that information is disclosed only to authorized individuals.

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

If an individual believes their records are not accurate, they can request corrections or the removal of material from the record by writing to DOI Privacy Office. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K.

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?

FAIR ISO and ISSO are responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ISO, the ISSO and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate Federal Acknowledgement Information Resource System (FAIR) Privacy Impact Assessment remedial activities are taken to mitigate any impact on individuals, in coordination with the IA APO.

GSA is responsible for Login.gov and the management and security of PII data submitted by individuals for identity verification and authentication purposes, as well as for reporting upon discovery any potential loss, compromise, unauthorized access, or disclosure of data resulting from their activities or management of the data that may impact partner agencies in accordance with Federal policy and established procedures.

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, FAIR follows Department of the Interior (DOI) incident response procedures to mitigate harm, assess impact, and ensure timely reporting and notification. Upon detection of a suspected or confirmed incident, immediate actions are taken to contain the breach, including isolating affected systems, securing compromised accounts, and preventing further unauthorized access. The incident is reported to the DOI Computer Incident Response Capability (DOI-CIRC) in accordance with DOI cybersecurity and privacy policies.

A risk assessment is conducted to determine the scope and impact of the breach, including the type of PII involved, the number of affected individuals, and the likelihood of harm. Based on this assessment, appropriate mitigation measures are implemented. If required, affected individuals will be notified in accordance with DOI breach notification policies and applicable federal laws and guidance. Notifications will include information about the nature of the breach, potential risks, and recommended protective actions.

The incident will also be reported to the DOI Senior Agency Official for Privacy (SAOP), the Departmental Privacy Office, and other oversight entities as required. All incidents are documented, and corrective actions are implemented to prevent reoccurrence.

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

The FAIR Privacy Impact Assessment (PIA) will be reviewed and updated on a regular basis to ensure continued accuracy and compliance with applicable privacy requirements.

At a minimum, the PIA will be reviewed annually as part of FISMA reporting and during system security and privacy authorization activities. In addition, the PIA will be updated whenever there are significant changes to the system, including modifications to system functionality, data collection practices, information sharing, or any changes that may impact privacy risks.

This ongoing review process ensures that privacy risks are continuously assessed and that appropriate safeguards remain in place throughout the system lifecycle.