U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Federal Acknowledgement Information Resource System (FAIRS)
Bureau/Office: Bureau of Indian Affairs, Office of Federal Acknowledgement
Date: April 29, 2025
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 445-0854
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The Bureau of Indian Affairs (BIA) completed a Privacy Threshold Analysis (PTA) on November 15, 2023, which concluded a Privacy Impact Assessment (PIA) was warranted. This PIA is being completed to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559), the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101), and Privacy Act of 1974, as amended (5 U.S.C. §552a).

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.

The new FAIRS is a cloud-based and cloud-hosted application designed to support OFA's activities which include reviewing and maintaining petition submissions for Federal Acknowledgement of American Indian Tribes.

Users of the system are only the OFA staff. User access is covered under the DOI Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment. For additional information on user authentication please see the EHI PIA on the DOI Privacy website: www.doi.gov/privacy/pia.

This is the initial PIA for FAIRS. It will be updated as the system is implemented to reflect any changes or processes and to address any identified privacy risks as OFA begins using the system.

C. What is the legal authority?

- Federal Acknowledgement of American Indian Tribes (25 CFR Part 83)
- Department of the Interior and Related Agencies Appropriations Act (43 U.S.C. 1457)
- Duties of Commissioner (25 U.S.C. 2 and 9)
- Government Organization and Employees (5 U.S.C. 301)
- Federally Recognized Indian Tribe List Act 1994 (Pub. L. 103-454)

D. Why is this PIA being completed or modified?

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

E. Is this information system registered on the Bison Governance, Risk, and Compliance (Bison GRC) platform?

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

UII Code: 010-000000018, Federal Acknowledgement Information Resource System (FAIRS), System Security and Privacy Plan (SSPP)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	Not Applicable	Not Applicable	Not Applicable

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

During the development of this PIA, the OFA identified the need to publish a new SORN to cover FAIRS 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*.

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.

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1076-0104, Federal Acknowledgement as an Indian Tribe, 25 CFR 83, Expires February 28, 2026. Per 25 CFR § 83.9 a response is required to obtain a benefit. The following forms are included in this information collection.

- BIA-8304, Individual History Chart
- BIA-8305, Ancestry Chart
- BIA-8306, Membership List

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Sex
☒ Birth Date
☒ Marital Status
☒ Other Names Used
☒ Spouse Information
☒ Mother's Maiden Name
☒ Child or Dependent Information

☒ Mailing/Home Address
☒ Other:

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, 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 Login.gov PIA at Login.gov_PIA_(Jan_2025).pdf (https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia)

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

☒ Individual (Petitioner)
☐ Federal agency
☒ Tribal agency

☐ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☒ Other: 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 Acknowledgement 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.

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

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

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

The PII collected is used by OFA in the performance of official functions to comply with 25 CFR Part 83, by applying anthropological, genealogical, and historical research methods to verify and evaluate a group's petition for Federal acknowledgment as an Indian Tribe.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Information may be shared with BIA employees acting in their official capacity in the performance of official functions to 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: *Describe the bureau/office and how the data will be used.*

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: *Describe the federal agency and how the data will be used.*

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.

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

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

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.

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

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

☒ 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.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

During the development of this PIA, the OFA identified the need to publish a new SORN to cover FAIRS 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*.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA.

Login.gov provides a link to its Privacy & Security page on both the sign-in and create account pages. Users may access the Login.gov Privacy & Security page on any web page of the site by clicking on the link in the footer. 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. The Login.gov PIA is available for review on the GSA PIA web page.

Before Login.gov shares any user PII with a partner agency, Login.gov acquires explicit consent from the user. The user must enter their password to provide that consent. Links to Login.gov Privacy Practices and Rules of Use are available to users before they create an account. The Login.gov Privacy Practices also links to the Login.gov Privacy Act Statement. Users may access the Login.gov Privacy Practices on any web page of the site.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

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.

☐ None

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

Records in FAIRS 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.

I. Will reports be produced on individuals?

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

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

☐ No

Section 3. Attributes of System Data

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

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.

Login.gov ensures the accuracy and completeness of the user's email address and 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.

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.

B. How will data be checked for completeness?

Once petitioners submit their records, OFA staff will check for completeness to determine whether the records comply 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.

Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts.

Login.gov collects PII directly from industry users who use the GSA identity authentication service to access FAIR. FAIR users are responsible for providing accurate information to GSA and must create a Login.gov account.

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

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

It is the responsibility of the petitioner to ensure the information provided is current.

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the accuracy of their records.

Login.gov collects PII directly from industry users who use the GSA identity authentication service to access FAIR. FAIR users are responsible for providing accurate information to GSA and must create a Login.gov account.

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

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

Records are covered by Indian Affairs Records Schedule (IARS) Records Series 3201-P5 – Acknowledgement 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 acknowledgement 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.

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

Data and information maintained within FAIRS is retained under the appropriate NARA approved IARS. Data dispositions follow NARA guidelines and approved records schedule for transfer, pre-accession, and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIA's records retention schedule. System administrators dispose of DOI records by shredding or pulping paper records and degaussing or erasing electronic records in accordance with NARA guidelines, Departmental policy, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Guidelines for Media Sanitization.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction) affect individual privacy.

There is a risk to the privacy of individuals due to the sensitive PII contained in FAIRS. FAIRS has undergone a formal Assessment and Authorization in accordance with the FISMA and NIST

standards. FAIRS 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. Only authorized personnel with proper credentials can access the records in the system. DOI requires multi-factor authentication (MFA) for network and system access. System access is based on least privilege access, role-based access controls and the "need-to-know." Access control lists were created and segmented, users cannot view information for other users unless specifically authorized. 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. Annually, employees, complete 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. 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. Physical, administrative, and technical controls are in place and other security mechanisms have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that FAIRS 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. Employees complete privacy training which includes topics on the collection and unauthorized

disclosure of information. 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. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, based on the "least privilege" principle. Access restrictions on data and various parts of the system's functionality are role-based and require supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. FAIRS meets BIA's information system security requirements, including operational and risk management policies.

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 petitioner submit their records, OFA staff check for completeness to determine whether the records comply 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 in accordance with an approved records retention schedule. The OFA is responsible for managing and disposing of BIA records in FAIRS 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, Acknowledgement Files. FAIRS 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 FAIRS 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 individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of privacy practices through this PIA. A SORN is in development for the FAIRS Program.

There is a risk that individuals may not receive adequate notice of the privacy practices of GSA (Login.gov). FAIR users access applications through authentication performed via Login.gov and are subject to the Login.gov Rules of Use. Login.gov provides users with links to its security practices and Privacy Act Statement. External FAIR users may review the GSA Login.gov PIA and the GSA/TTS–1 (Login.gov) SORN for details on the collection, use, storage, or sharing of their PII by GSA.

GSA is responsible for protecting the data collected and processed on Login.gov. Login.gov manages security through the auditing of access, vetting of privileged users, and enforcing the principle of least privileged access. By keeping all audit logs for any action taken as a privileged user on Login.gov systems, there is a detailed history maintained to determine who made changes and when. By using background check investigations for privileged users and individuals with access to user PII, Login.gov seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining the least privileged access, Login.gov restricts access to FAIR to the minimum required levels, decreasing the risk of unauthorized disclosure or abuse. Additionally, all these managerial controls are subject to regular review. Login.gov's physical security is provided by its FedRAMP-authorized cloud service provider. Login.gov manages technological security via a defense-in-depth approach, minimizing access at every level, with strong encryption of data both in transit and at rest. Additionally, other services run on top of Login.gov to further detect any compromised systems, atypical system behavior, and/or data disclosure.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. FAIRS is hosted and administered within a DOI-approved and Federal Risk and Authorization Management Program (FedRAMP) certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP authorization to operate (ATO). The provider will be required to submit additional security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information in accordance with Federal and DOI privacy and security standards.

In addition to the risk mitigation actions described above, the BIA maintains an audit trail of activity sufficiently enough to reconstruct security relevant events. The BIA follows the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI network requires 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 initially and 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.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of the system and data collected is relevant and necessary to the purpose for which FAIRS was designed and supports the Indian Affairs mission of OFA to comply with and implement 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.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No: FAIRS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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

☐ Yes: *Explanation*

☒ No: FAIRS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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

☐ Yes: *Explanation*

☒ No: FAIRS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

E. How will the new data be verified for relevance and accuracy?

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

F. Are the data or the processes being consolidated?

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

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

☒ No: No data or processes are being consolidated.

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

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

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

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 FAIRS 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.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes.

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)

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No: The system will not use new technologies in ways DOI has not previously employed.

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

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

Login.gov logs monitor all user actions. Users may review the Login.gov PIA for additional information.

☐ No

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

The FAIRS system is not intended to monitor individuals. However, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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. Users may review the Login.gov PIA for additional information.

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

FAIRS 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 FAIRS 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.

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 FAIRS 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.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. The system also inherits controls from Login.gov for authentication. The Login.gov PIA describes the physical controls implemented by GSA to protect information processed using the service. The Login.gov PIA may be seen at Login.gov_PIA_(Jan_2025).pdf (https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia)

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. The Login.gov PIA describes the technical controls implemented by GSA to protect information processed using the service. The Login.gov PIA may be seen at

Login.gov_PIA_(Jan_2025).pdf (https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia)

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. The Login.gov PIA describes the administrative controls implemented by GSA to protect information processed using the service. The Login.gov PIA may be seen at Login.gov_PIA_(Jan_2025).pdf (https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia)

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Deputy Associate Chief Information Officer serves as the Information System Owner (ISO) for FAIRS. 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 FAIRS. 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 IA APO.

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.

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

FAIRS 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

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.