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: Solution Trust Accountability Tracker (STAT)
Bureau/Office: Bureau of Indian Affairs (BIA), Office of Trust Services (OTS)
Date: December 15, 2023
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

☒ Members of the general public
☒ Federal personnel and/or Federal contractors
☐ Volunteers
☐ All

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

B. What is the purpose of the system?

The BIA completed a Privacy Threshold Analysis (PTA) on June 28, 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 (5 U.S.C. § 552a).

The Bureau of Indian Affairs Office of Trust Services carries out Indian Affairs trust responsibilities to Indian tribes, individuals and oversees all activities associated with the management and protection of trust and restricted lands, natural resources, and real estate services. The office provides land-related functions to Indian trust owners including acquisition, disposal, rights-of-way; leasing and sales, and assists them in the management, development, and protection of trust land and natural resource assets. Programs administered by the Office of Trust Services include real estate services; land title and records; probate; natural resources; forestry and wildland fire management; irrigation, power, and safety of dams.

BIA-STAT is a Federal Risk and Authorization Management Program (FedRAMP) approved Moderate Impact – Software as a Service (MI-SaaS) cloud solution. It is an advanced project management suite/collaborative environment managed by the Office of Trust Services (OTS). BIA-STAT is a tool used to enhance workforce management practices, maximize productivity and efficiency at both a staff and program level. This solution is used within OTS for a variety of programs needing to track the completion of various internal projects and program documentation.

The BIA-STAT uses Active Directory (AD) authentication. AD authentication for 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.

C. What is the legal authority?

- The Public Land Act of 1796 (1 Stat. 464)
- Surveying duties (43 U.S.C. 52)
- Rules of survey (43 U.S.C. 751)
- Navigable rivers as public highways (43 U.S.C. 931)
- Public information; agency rules, opinions, orders, records, and proceedings (5 U.S.C. 552)
- Departmental regulations (5 U.S.C. 301)
- Duties of Secretary (43 U.S.C. 1457)
- Records management by agency heads; general duties (44 U.S.C. 3101 et seq.)
- Indian Long-Term Leasing Act of 1955 (25 U.S.C. Sec. 415 (h))
- Federal Property and Administrative Services Act (40 USC Section 471 et seq.)
- Excess real property located on Indian reservations (40 USC Section 523)
- Federal Management Regulation, Subchapter C – Real Property, part 102-72
- Indian Reorganization Act of 1934 (IRA) (25 U.S.C. § 5110)
- Indian Self-Determination Act of 1975 (ISDEAA) (Pub. L. 93-638)
- Title 31 U.S.C. §§ 1104 - 1113, the Budget Process
- Indian Dams Safety Act of 1994 (Pub. L. 103-302, 25 U.S.C. § 3801 et seq.)
- Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission and Execution of the Budget*.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review

□ Merging of Systems
□ Significantly Modified Information System
□ Conversion from Paper to Electronic Records
□ Retiring or Decommissioning a System
□ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: Xacta 360 ID: BIA-0031-SYS; UII Code: 010-000000077
□ 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)*

BIA-STAT is not a Privacy Act system of record as defined at 5 U.S.C. 552a (5).

Records in BIA-STAT pertaining to individuals who require access to Departmental networks, information systems, and e-mail services are maintained under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021), which may be viewed at https://www.doi.gov/privacy/doi-notices.

BIA employee names and work email addresses may be used to assign or collaborate on tasks and projects via a BIA-STAT tracking workflow. BIA-STAT tracking workflows are used to manage the completion of various internal projects and the processing of program documentation. This information is obtained from the employee being assigned a task or project or from BIA employee directories, which are maintained under SORN INTERIOR/DOI-58, Employee Administrative Records published 64 FR 19384 (April 20, 1999); modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021).

BIA-STAT may include the name of a Tribal member requesting the processing of, or the status of documentation being processed by OTS. This information is extracted from documents maintained under INTERIOR/BIA-04, Trust Asset and Accounting Management System (TAAMS) published 79 FR 68292 (November 14, 2014), modification published 86 FR 50156 (September 7, 2021), which may be viewed at https://www.doi.gov/privacy/doi-notices.

□ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: Name and work email address of BIA employees and contractors assigned tasks and projects tracked BIA-STAT. Name of Tribal members requesting the processing of, or status of documentation being processed by OTS. Name and email address of Tribal entities; however, only records containing personal information relating to individuals is subject to the Privacy Act. User (login) names and government email addresses are recorded for BIA employees and contractors who are authorized users of BIA-STAT.

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

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

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?

BIA-STAT uses BIA employee and contractor name and work email address to assign tasks and projects tracked in BIA-STAT. Name and work email addresses of Tribal officials or names of Tribal members is used to provide the status of documentation being processed by OTS. User (login) names and government email addresses are recorded for BIA employees and contractors who are authorized users of BIA-STAT.

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 in BIA-STAT may be shared with BIA employees (employees and contractors) who have a need-to-know in the performance of their official duties to manage and track progress of assigned projects and tasks.

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

Bureau of Land Management will have access to cadastral survey land tracking information to provide survey timeframes, cost estimates and other related information. This information does not include PII.

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
☐ 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 contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support.

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

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

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☒ No: BIA-STAT data is not collected directly from individuals.

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.*
☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and related SORNS published in the Federal Register. Federal personnel receive privacy notices before logging onto government computers and BIA-STAT. More information about the Department's privacy program including compliance documents and how to submit a request for agency records pertaining to you is available at DOI's Privacy website at https://www.doi.gov/privacy.

☐ Other: *Describe each applicable format.*
☐ 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 BIA-STAT are retrieved by case, project, or tracking number.

I. Will reports be produced on individuals?

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

Reports are not produced on individual but are produced on the status of assigned tasks or projects. However, BIA-STAT can produce user reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit Logs also collect information on system users such as username. System administrators and the information system owner have access to these activity reports.

□ No

Section 3. Attributes of System Data

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

Data will not be collected from sources other than DOI records. Data is checked for accuracy by an employee at the time it is entered into BIA-STAT. Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

B. How will data be checked for completeness?

Data is checked for completeness by an employee at the time it is entered into BIA-STAT. 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.

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

Data is checked for currency, by an employee at the time it is entered into BIA-STAT. 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.

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

BIA-STAT records are maintained per the Departmental Records Schedule (DRS), DAA-0048-2013-0001, Short-term Administrative Records. Records under this schedule are considered temporary and may be destroyed three years after cut-off. These records encompass administrative functions that are produced and maintained during routine business, and do not reflect government business that is subject to additional preservation. Records are characterized by being necessary for day-to-day operations but not long-term justification of the office's activities.

Information technology records are maintained under the DRS 1.4 Information Technology (IT) (DAA-0048-2013-0001-0013, System Maintenance and Use Records and DAA-0048-2013-0001-0014, System Planning, Design, and Documentation). 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 a temporary disposition and will be cut off when superseded by a newer version or upon termination of the system and destroyed three years after cut-off.

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

Data disposition 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 Fund 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 for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

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.

Although BIA-STAT is hosted in a FedRAMP approved Moderate Impact – Software as a Service (MI-SaaS) cloud solution, there is a low risk to the privacy of individuals because of the limited, non-sensitive PII used in BIA-STAT. The system will undergo a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards the required management, operational, and technical controls established by NIST Special Publication 800- 53, Security and Privacy Controls for Information Systems and Organizations will be implemented 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 unauthorized 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. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access is based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages BIA-STAT user accounts using the Bison System Access Management (BSAM) system. 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 is officially employed until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable BIA-STAT user accounts. System administrators use 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 of unauthorized access or scanning of the system is reported to IT Security. Physical, operational, and technical controls are in place and other security mechanism 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. Audit logs are routinely checked for unauthorized access or system problems. 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 BIA-STAT 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 not authorized access and to review 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 to data and various parts of the system’s functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. BIA-STAT meets BIA’s information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. Data is checked for accuracy, currency, and completeness by an employee at the time it is entered into BIA-STAT.

There may be a risk associated with the collection of information from other DOI systems. There is a minimal risk associated with the collection of the limited, nonsensitive PII data elements from TAAMS. The risk is mitigated because it is the responsibility of the system owners of internal systems to ensure data maintained is accurate. TAAMS data is verified by one of the following: 1) Individuals or Tribes verify that information is accurate; 2) Supporting documentation is required for data verification such as birth certificates, divorce decrees, certificates of death, and signed affidavits; 3) Data entered in TAAMS by BIA is subject to internal system validation based on preprogrammed business rules developed from a process known as Business Process Reengineering (BPR). For example, a date of birth or date of death cannot be in the future. Additionally, validation against internal business rules and existing land trust deeds and records is conducted.

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 OTS, as the information owner, is responsible for managing and disposing of BIA records in BIA-STAT. The OTS ensures only records needed to support its program, Tribes, and Tribal members is maintained. The OTS maintains the records until no longer needed for business use. When the business function determines they are no longer needed for use within BIA-STAT, they are combined with the appropriate program records and then transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA. The tracking records in BIA-STAT are maintained per the Departmental Records Schedule (DRS), DAA-0048-2013-0001, Short-term Administrative Records. Records under this schedule are considered temporary and may be destroyed three years after cut-off. These records encompass administrative functions that are produced and maintained during routine business, and do not reflect government business that is subject to additional preservation. Records are characterized by being necessary for day-to-day operations but not long-term justification of the office’s activities.

Information technology records are maintained under the DRS 1.4 Information Technology (IT) (DAA-0048-2013-0001-0013, System Maintenance and Use Records and DAA-0048-2013- 0001-0014, System Planning, Design, and Documentation). 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 a 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. Information collected and stored within BIA-STAT is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published INTERIOR/BIA-04, Trust Asset and Accounting Management System (TAAMS) published 79 FR 68292 (November 14, 2014), modification published 86 FR 50156 (September 7, 2021) and records pertaining to Departmental networks, information systems, and e-mail services are maintained under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021), which may be viewed at: https://www.doi.gov/privacy/sorn.

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. BIA-STAT is hosted and administered within a DOI-approved and FedRAMP-certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP certification. The data residing in the system is backed up on a nightly basis. BIA manages BIA-STAT 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 walks in the DOI door until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable BIA-STAT user accounts.

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 two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST SP 800-53.

DOI employees must take Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management, Section 508 Compliance, and Controlled Unclassified Information (CUI) training before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The use of the system and data collected is relevant and necessary to the purpose for which BIA- STAT was designed and supports the Indian Affairs (IA) mission of being responsive to customer inquiries about documentation being processed by BIA.

☐ No

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

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

☒ No

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

□ Yes: *Explanation*
☒ No

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

□ Yes: *Explanation*
☒ No

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

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

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

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 on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages BIA-STAT 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 walks in the DOI door until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable BIA-STAT 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.

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

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The Privacy Act contract clauses Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984) and FAR 52.224-2, Privacy Act (Apr 1984) were included in the contract. The Privacy Act contract clauses FAR 52.224-3, Privacy Act Training (Jan 2017) and FAR 52.239-1, Privacy or Security Safeguards (Aug 1996) will be included as a modification to the contract.

☐ No

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

☐ Yes. *Explanation*
☒ No

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

☒ Yes. *Explanation*

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

☐ No

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

The BIA-STAT 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.

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

BIA-STAT 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 BIA-STAT Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management, Section 508 Compliance, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.

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

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
□ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
□ Cipher Locks
☒ Identification Badges
□ Safes
☒ Combination Locks
☒ Locked Offices
□ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Multi-Factor Authentication (MFA)
☒ Firewall
☒ Encryption
☒ User Identification
□ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. Multifactor tokens

(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. *Describe*

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

The Associate Chief Information Officer serves as the Information System Owner (ISO) for BIA-STAT. 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 Indian Affairs information processed and stored by BIA-STAT. 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 Associate Privacy Officer (APO).

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

The BIA-STAT 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 to individuals, in coordination with the IA APO.