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: Identity Information System (IIS) – eProfile Database
Bureau/Office: Bureau of Indian Affairs/ Office of Information Management Technology (OIMT)
Date: September 27, 2022
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 Identity Information System (IIS) is a government-off-the-shelf (GOTS), major application developed by the Bureau of Indian Affairs (BIA) Office of Information Management Technology (OIMT). IIS is comprised of two separate modules supporting business processes within the Assistant Secretary – Indian Affairs (AS-IA), the Bureau of Indian Affairs (BIA), and Bureau of Indian Education (BIE) (collectively referred to as Indian Affairs (IA)). IIS serves as an automated tool for tracking background security screening and information system access

requests and authorizations. This privacy impact assessment is limited to the IIS e-Profile data entry module.

The IIS e-Profile data entry module facilitates the management of information about actively employed IA Federal employees and contractors. The data maintained is used to manage and track information system access requests and authorizations. Information maintained about individuals includes work contact information, office of assignment, office location, supervisor name, and information related to information system access requests. System managers, business owners, and system administrators use the system to process requests to IA information systems. The system tracks system access requests and records the system manager's response to the request, including the approval and disapproval of the request. After the departure of staff from IA employment, the system allows the manager to initiate the revocation of system access privileges of the separated individual.

The IIS 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?

Departmental Regulations (5 U.S.C. 301); Federal Information Security Act (Pub. L. 104-106, section 5113); Homeland Security Presidential Directive-12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, Section 3001 (50 U.S.C. 435b); Federal Property Regulations, July 2002; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105–277); Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource.

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:

UII Code:010-000002646, Identity Information System (IIS) System Security and Privacy Plan

☐ 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	N/A	No	N/A

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

☒ Yes: AD user access records in IIS are maintained under DOI system of records notices: 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. Some legacy records may be covered under INTERIOR/DOI-45, Personnel Security Program Files, 87 FR 54242 (September 2, 2022).

☐ 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
☒ Birth Date
☒ Social Security Number (SSN)
☒ Other: Work contact information: phone/fax/cell phone number, office, duty location. Government Approver/Supervisor Full Name, work phone number, and work email address.

The legacy records contain Dates of Birth and Social Security Number (SSN) in eProfile. The DOB and SSN ceased to be collected or input into eProfile August 2020. The authority used to solicit the SSN was Executive Order (EO) 9397, as amended by EO 13478.

The reason for past collection of the SSN was to identify records unique to the individual associated with another database. This association is no longer needed so the SSN and DOB are no longer collected. Access to this data is limited to authorized system administrators in the performance of official duties. The legacy data will be archived with the appropriate safeguards and disposed of in accordance with the approved records schedule. Access to this data is limited to authorized system administrators in the performance of official duties.

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: Employees provide work-related contact information directly into eProfile when the information needs updating.

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: Information collected on employees and contractors is input by government supervisors, managers, and Contracting Officer Technical Representatives (COTR).

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

PII is used to manage and track information system access requests and authorizations to ensure appropriate security access controls are implemented and monitored. The intended uses of the PII collected and maintained in IIS eProfile is to create a User record, initiate and approve information system account authorizations, and to grant access to IA information systems.

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

☒ Within the Bureau/Office: Helpdesk personnel have access to all employee's work information which includes name, title, work phone, employee type, organization name, organization code, work address, list of systems an employee is authorized to access, role (User, Supervisor, COTR) and supervisor's name and can retrieve an employee's record using an employee's name, office name, and organization code. The intended uses of the PII are to create a User record, initiate and approve information system account authorizations, and to grant access to IA information systems. Supervisors and COTRs can view work information of those employees they manage. This information includes name, title, work phone, email address, employee type, organization name, organization code, work address, list of systems an employee is authorized to access, role (User, Supervisor, COTR) and supervisor's name and can retrieve an employee's record using an employee's name, office name, and organization code. The intended uses of the PII are to create a User record, initiate and approve information system account authorizations, and to grant access to IA information systems.

☒ Other Bureaus/Offices: Information may be shared with the Department, as required by law and policy, to report and respond to potential security incident or to investigate violation of law, regulation, and policy.

☒ Other Federal Agencies: Information may be shared with other agencies, as required by law and policy, to report and respond to a potential security incident or to investigate violation of law, regulation, and policy.

☐ Tribal, State or Local Agencies:

☒ Contractor: Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support for IIS. Contractors also provide system and database management support. Contractors do not have access to sensitive PII.

☐ Other Third-Party Sources:

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

☒ Yes: Providing information when onboarding is voluntary, however, failure to provide requested information may result in denial of access to the Department of the Interior (DOI) networks and information systems.

☒ No: Work contact information is not obtained directly from the employee or contractor for entry into eProfile but from DOI records. After initial input, employees may update their own information.

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

☒ Privacy Act Statement: A Privacy Act Statement (PAS) is presented to employees. The PAS provides detailed information on the authority and purpose of collecting PII, how PII is used and with whom the PII is shared, the applicable routine uses under INTERIOR/DOI-45, Personnel Security Program Files SORN, and the voluntary nature of the collection, as well as impacts for not providing information.

☒ Privacy Notice: Privacy notice is provided through publication of this privacy impact assessment and the published INTERIOR/DOI-45, Personnel Security Program Files SORN, which may be viewed at https://www.doi.gov/privacy/sorn.

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

☐ None

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

- Employees can view their own work-related, User data in eProfile. Data includes name, title, work phone, employee type, organization name, organization code, work address, list of systems an employee is authorized to access, role (User, Supervisor, COTR) and supervisor's name.

- Helpdesk personnel have access to all employee's work information which includes name, title, work phone, employee type, organization name, organization code, work address, list of systems an employee is authorized to access, role (User, Supervisor, COTR) and supervisor's name and can retrieve an employee's record using an employee's name, office name, and organization code.
- Supervisors and COTRs can view work information of those employees they manage. This information includes name, title, work phone, email address, employee type, organization name, organization code, work address, list of systems an employee is authorized to access, role (User, Supervisor, COTR) and supervisor's name and can retrieve an employee's record using an employee's name, office name, and organization code.

I. Will reports be produced on individuals?

☒ Yes: eProfile reports are role based. Reports can be created to identify who has access to an information system and for other managerial purposes. 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 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?

Supervisors and COTRs are responsible for ensuring information provided is accurate. Verification of the data collected from DOI records is the responsibility of the supervisors and COTRs. Users have direct access to their profile and are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

Employees can seek records about themselves that are maintained in this system of records and if the individual believes the records are not accurate can request corrections or the removal of material from the record by writing to the System Manager identified in the SORN INTERIOR/DOI-45, Personnel Security Program Files. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

B. How will data be checked for completeness?

Supervisors and Users are responsible for ensuring information provided is complete. Various operational reports can be generated by administrators and supervisors which list missing information for any portion of the employee/contractor records such as training, invalid office, or location data, missing mandatory training data, etc. This report is used to ensure data maintained in IIS is complete. 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.

Employees can seek records about themselves that are maintained in this system of records. And if the individual believes the records are not complete can request corrections or removal of material from the record by writing to the System Manager identified in the SORN INTERIOR/DOI-45, Personnel Security Program Files. These rights and request 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).

Supervisors and COTRs are responsible for ensuring information provided is current. Supervisory reports can be generated to review IIS data to assist in discovering inaccurate information, which can be updated by the supervisor. 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.

Employees can seek records about themselves that are maintained in this system of records. And if the individual believes the records are not current can request corrections or the removal of material from the record by writing to the System Manager identified in the SORN INTERIOR/DOI-45, Personnel Security Program Files. These rights and request requirements are outlined in the DOI Privacy Act regulation 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.

The OIMT staff are responsible for ensuring records are retained and disposed of in accordance with the Departmental Records Schedule (DRS)-4.1. They are Long-term Administration Records (DAA-0048-2013-0001-0002). The disposition of these records is temporary and the retention period, 7 years, begins when an individual separates from IA.

IIS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the National Archives and Records Administration (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 cut-off. Information collected and stored within IIS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

System Planning, Design, and Documentation are maintained under Departmental Records Schedule (DAA-0048-2013-0001-0014). Records include IT files that are necessary for day-to-day operations but no long-term justification of the office's activities. 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?

IIS records are retained under the appropriate NARA approved Department Records Schedule. 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 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.

There is a moderate risk to the privacy of individuals due to the sensitive PII maintained in IIS. The system has undergone 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. IIS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST Special Publication 800-53, Security and Privacy Controls for Federal 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. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access are based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. System administrators use 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. Annually, employees, complete privacy 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, 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 IIS 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. The eProfile module's legacy records contain DOB and SSNs. The DOB and SSN stopped being collected or input into eProfile August 2020, to further reduce the risk and is in line with the policy to only collect the minimal amount of information needed to perform official functions for which the system was designed. The reason for collecting the SSN in the past was to identify records unique to the individual associated with another database. The IA recognized the risk to individuals; therefore, the new system will no longer collect this information. The legacy data will be archived with the appropriate safeguards and disposed of in accordance with the approved records schedule.

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. IIS meets IA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information on users. This risk is mitigated through established verification procedures to validate that the information submitted is accurate and complete. Also, it is the individual's responsibility to ensure the information they submit on employment forms is accurate. Users can view their own work-related data in eProfile and can contact their Supervisor or COTR and have outdated or incorrect information updated.

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 Office of Information Management Technology staff are responsible for ensuring records are retained and disposed of in accordance with the Departmental Records Schedule (DRS)-4.1. They are Long-

term Administration Records (DAA-0048-2013-0001-0002). The disposition of these records is temporary and the retention period, 7 years, begins when an individual separates from BIA.

IIS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the National Archives and Records Administration (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 cut-off. Information collected and stored within IIS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy, and NARA guidelines. Copies of records approved for destruction are disposed of by shredding or pulping for paper records, records on electronic media are degaussed or erased in accordance with applicable NARA Guidelines, Department Policy, Department and/or Indian Affairs Records Schedules, and the National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitization.

There is a risk that individuals may not have adequate notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through the PAS, this PIA and through the published DOI SORN DOI-45, Personnel Security Program Files, 87 FR 54242, September 2, 2022, which may be viewed at: https://www.doi.gov/privacy/sorn. This notice provides information to individuals on how their PII will be used and shared and how they may seek notification, access, or amendment of their records. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

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 Training (IMT) which includes topics on Cybersecurity, Privacy, Records Management, Paperwork Reduction Act, and Controlled Unclassified Information 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 they understand their 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: IIS is an automated tool to track information system access requests and authorizations. The use of the system and data collected is relevant and necessary to the purpose for which IIS was designed and supports the Indian Affairs mission.

☐ No

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

☐ Yes
☒ No

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

☐ Yes
☒ No

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

☐ Yes
☒ No

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

Not Applicable. IIS 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.
☐ Yes, processes are being consolidated.
☒ 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*

IIS users are given access to data on a 'least privilege' basis and a need-to-know to perform specific official functions. Data resides in multiple tables and limits users' access by organizational role and responsibility related to their IIS assigned role. eProfile allows an active

employee, contractor, or an individual with IA affiliation to review information maintained in their own individual record.

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

To gain access to IIS eProfile, the individual must be an active employee or contractor or individual working within the umbrella of IA; have a favorable background investigation determination, completed the initial DOI security awareness training; and have accepted the DOI Rules of Behavior. Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. IA manages user accounts using the IIS eProfile, a self-contained system that provides workflow and access control support, which includes establishing, activating, modifying, reviewing, disabling and removal of 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: Contractors are involved in the design and development of the system. Privacy Act clauses are included in all contractor agreements. Contractors are required to sign nondisclosure agreements as a contingent part of their employment, sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. 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
☒ No

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

☒ Yes. The purpose of IIS 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?

IIS is not designed 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 for security purposes. 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?

IIS can audit the usage activity in 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. IIS assigns roles based on the principles of 'least privilege' and performs 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 IIS audit trail will include a user's Person ID, 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
☒ Firewall
☒ Encryption

☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(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 Deputy Associate Chief Information Officer serves as the Information System Owner (ISO) for IIS. 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 IIS. 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 IIS 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.