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: Indian Education-Network Infrastructure (IE-NI)
Bureau/Office: Bureau of Indian Education (BIE)
Date: December 17, 2020
Point of Contact
Name: Richard Gibbs
Title: 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 Indian Affairs (IA) Bureau of Indian Education (BIE) school system is comprised of 187 schools that are located in 23 states, a central office with operations in Washington, DC, and Albuquerque, NM; and Education Line Offices (ELO) throughout the country. There are approximately 47,000 students enrolled in IA schools and dormitories nationwide. BIE is different from other educational jurisdictions in that BIE operates in 23 states and is required by statute to report by school to State and Federal education agencies.

The Indian Education Network Infrastructure (IE-NI) General Support System (GSS) is a Wide Area Network (WAN) which provides network access and Internet connectivity to BIE schools, offices, and universities, adult education learning centers, juvenile detention centers, and Tribally Controlled Community Colleges (TCCCs). IE-NI provides a centralized network infrastructure to support Native American communities through lifelong learning. IE-NI is a data transport WAN, comprised of only data transport and network infrastructure components. IE-NI does not process nor store data on individuals, it transports packets of data segments and provides the network infrastructure that enables connection between BIE educational locations and the Internet.

C. What is the legal authority?

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); the E-Government Act of 2002 (Pub. L. 107-347); the Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; The Snyder Act of 1921 (Pub. L. 67-85); Indian Reorganization Act of 1934 (Pub. L. 73-383), Indian Self-Determination and Education Assistance Act of 1975 (Pub. L. 93-638); Education Amendments of 1978 (Pub. L. 95-561), Every Student Succeeds Act (Pub. L. 114-95); Native American Education Improvement Act of 2001 (Pub. L. 107-110).

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: *Enter the UII Code and the System Security Plan (SSP) Name*

☒ No. IE-NI is undergoing the registration process for CSAM.

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.*

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)*

☒ No

IE-NI is not a Privacy Act system of records. However, login records related to accessing the network is covered under the DOI system of records notice DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, which may be viewed at https://www.doi.gov/privacy/doi-notices.

Due to the nature of the IE-NI as a WAN, there are data packets transported by IE-NI that may include PII in applications supported by IE-NI. These records are under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for meeting the requirements of the Privacy Act for the collection, maintenance and sharing of their records including publishing systems of records notices and addressing requests for notification, access or amendment under the Privacy Act.

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: Username, User ID, Password, Work Email Address, Work Phone Number for network access purposes. IE-NI does not collect or store PII beyond login information. It transports data packets throughout the IE-NI network for the applications served by IE-NI which may include PII. BIA separately assesses the PII handling activities and addresses the identified privacy risks of individual applications that IE-NI supports. Please see the DOI Privacy Program website at https:///www.doi.gov/privacy/privacy-program for PIAs and related SORNs for these individual applications.

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
☒ Other: IA tracks and maintains IE-NI user accounts via the Identity Information System (IIS), a self-contained system that provides workflow and access tracking, which includes recording of activation, modification, review and deletion of IE-NI user accounts. All account processes are manual, not automated. User data is provided by individual users during the account creation or updating process. Initial information is collected by Human Resources or the Contracting Officer Representative (COR) from individuals during the employment on-boarding process.

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

The primary use of the limited PII is to authenticate users accessing the IE-NI network infrastructure remotely through the Virtual Private Network and to authenticate administrative users operating and managing the IE-NI network infrastructure. The information is used to specify a username, user account and temporary password during user account creation. IE-NI does not collect or store PII beyond login information. It transports data packets throughout the IE-NI network for the applications served by IE-NI. BIA separately assesses the PII handling activities and addresses the identified privacy risks of individual applications that IE-NI supports. Please see the DOI Privacy Program website at https:///www.doi.gov/privacy/privacy-program for PIAs and related SORNs for these individual applications.

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.*

IE-NI does not collect or store the PII it transports. Information may be shared with BIA employees acting in their official capacity in the performance of official functions to review and analyze audit records for indications of inappropriate or unusual activity and report findings to designed personnel.

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

For incident response management purposes, the data packets transmitted through IE-NI may be intercepted and analyzed by authorized officials within BIA. This activity is coordinated with the affected bureau or office who owns and manages the data for its systems, applications and programs. Any PII or data collection is handled by the bureau that owns/manages that data in accordance with any agreements they may have in place for internal or external communications, and DOI security and privacy policies.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

For incident management and computer security management purpose, some information - network routing information from external sources might be shared with the Department of Homeland Security or other pertinent federal agencies in accordance with legal authority.

☐ 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.*

User information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support and as authorized pursuant to the routine uses contained in DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, which may be viewed at https://www.doi.gov/privacy/doi-notices. Contractors have access to the systems and applications on IE-NI as authorized to perform their official duties.

☐ 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.*

Information required to create the individual's user account is provided by an individual's supervisor or COR, which is derived from documents submitted during the employment on-boarding process. These forms provide the requisite Privacy Act Statement informing the individual that providing the information is voluntary and that the consequences of not providing the information may impact employment. However, IE-NI does not collect information directly from individuals for data packets that are transported.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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.*

Privacy notice is provided through publication of this privacy impact assessment and the published DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS),

72 FR 11040, March 12, 2007, which may be viewed at https://www.doi.gov/privacy/doi-notices.

☒ 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.

☐ 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 IE-NI are primarily retrieved by name, username, and workstation name. Retrieval is limited to system administrators.

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 username. System administrators also conduct annual user account reconciliation which is manually performed comparing IE-NI system account information against account creation or deletion in IIS. 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?

IE-NI does not collect or store PII beyond login information. It transports data packets throughout the IE-NI network for the applications served by IE-NI. BIA separately assesses the PII handling activities and addresses the identified privacy risks of theses individual applications that IE-NI supports. Please see the DOI Privacy Program website at https:///www.doi.gov/privacy/privacy-program for PIAs and related SORNs for these individual applications.

The purpose of the IE-NI is to provide a conduit for BIE network traffic. As such, IE-NI does not ensure that data which traverses the network is accurate.

User account information is provided directly by the User during account creation and can be updated by the User as the need arises. Users are responsible for the accuracy of their data. Additionally, system administrators conduct annual user account reconciliation which is manually performed comparing IE-NI system account information against account creation or deletion in Identity Information System to verify data accuracy. The BIA Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

B. How will data be checked for completeness?

Users are responsible for the completeness of their data. User account information is provided directly by the User during account creation and can be updated by the User as the need arises. Additionally, system administrators conduct annual user account reconciliation which is manually performed comparing IE-NI system account information against account creation or deletion in Identity Information System to ensure data is complete. The BIA ISCMP specifies the review, monitoring and assessment frequency of all NIST SP 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

The purpose of the IE-NI is to provide a conduit for BIE network traffic. As such, IE-NI does not ensure that data which traverses the network is complete.

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

Users are responsible for ensuring their data is current. User account information is provided directly by the User during account creation and can be updated by the User as the need arises. Additionally, system administrators conduct annual user account reconciliation which is manually performed comparing IE-NI system account information against account creation or deletion in Identity Information System to ensure data is current. The BIA ISCMP specifies the review, monitoring and assessment frequency of all NIST SP 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

The purpose of the IE-NI is to provide a conduit for BIE network traffic. As such, IE-NI does not ensure that data which traverses the network is current.

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

System administration records are maintained under the Departmental Records Schedule (DRS)-4.1, 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 bureaus/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 cut-

off. 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.

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

The Indian Affairs' Employee Exit Clearance policy outlines supervisor procedures and responsibilities to remove information when employees and contractors leave the bureau. Records management policies and procedures govern disposal of information. 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 Funds Administration (BTFA), Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIE's records retention schedule. Approved disposition methods for records include shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and 384 Departmental Manual 1.

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 PII that may be in data packets transported in IE-NI. IE-NI 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. IE-NI is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 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.

IE-NI is a conduit for BIE network traffic and is subject to security controls implemented in accordance with NIST 800-53 and the BIA ISCMP to protect the IE-NI environment. The security controls include monitoring the IE-NI network traffic for malicious activities, data loss prevention, and security incidents.

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" in order to complete assigned duties. BIA manages IE-NI user accounts using IIS, which includes establishing, activating, modifying, reviewing, disabling and removal of IE-NI 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 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. 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, protecting against inappropriate use or disclosure to unauthorized individuals.

There is a risk information that IE-NI 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 in order 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. IE-NI meets BIA’s information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. This risk is mitigated as system administrators conduct annual user account reconciliation which by comparing IE-NI system account information against account creation or deletion in Identity Information System to ensure the information is accurate. The BIA Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all National Institute of Standards and Technology (NIST) 800-53 security and privacy controls to maintain the integrity and accuracy of the data. Additionally, Users are responsible for ensuring their data is current. User account information is provided directly by the User during account creation and can be updated by the User as the need arises.

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. In regard to information handling and retention procedures, the Office of Information Management Technology (OIMT) is responsible for managing and disposing of BIA records in IE-NI as the information owner. THE OIMT ensures only records needed to support its program, Tribes, and Tribal members is maintained. Information collected and stored within IE-NI 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 DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, which may be viewed at: https://www.doi.gov/privacy/doi-notices. Additionally, Privacy Act Statements (PAS) are included on the onboarding forms (.e.g., OF 306, Declaration for Federal Employment and SF-85P, Questionnaire for Public Trust Positions). 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 maintained 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 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, 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 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 IE-NI was designed and supports the Bureau of Indian Education's mission. IE-NI provides data packet transport and a network infrastructure that enables connection between BIE educational locations and the Internet.

☐ 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. IE-NI 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: Individual users have access to their own data. Auditors or BIA risk management team may access the system at least annually or as described in the ISCMP.

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 IE-NI user accounts using IIS, which includes establishing, activating, modifying, reviewing, disabling and removal of IE-NI 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 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

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

☒ Yes. *Explanation*

The purpose of IE-NI 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 IE-NI 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 Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

IE-NI has the ability to 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, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. IE-NI 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. IE-NI assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to DOI Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and role-based privacy training 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 sufficiently to reconstruct security relevant events. The IE-NI 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
- ☒ 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 Associate Chief Information Officer (ACIO) is the IE-NI Information System Owner (ISO). The ISO, Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in IE-NI. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act

complaints and requests for notification, access, redress, or amendment of records in consultation with the DOI Privacy Officials.

For the applications hosted by IE-NI the data is under the control of each system owner who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including responding to Privacy Act requests for access, and amendments, as well as processing complaints in consultation with privacy officials.

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 IE-NI ISO and ISSO are responsible for the central oversight and management of the IE-NI 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 IE-NI ISO, ISSO, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.

For applications hosted by IE-NI, the data is under the control of each system owner who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including the reporting the loss, compromise, unauthorized disclosure or access of individuals' personal information, in consultation with privacy officials.