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: Web Education Transportation (WebET 2.0)
Bureau/Office: Bureau of Indian Education, School Operations
Date: August 9, 2024
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 445-0854
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The Bureau of Indian Affairs (BIA), Office of Information Management Technology (OIMT) completed a Privacy Threshold Analysis (PTA) December 20, 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.

The WebET 2.0 is a cloud-based, contractor-owned, contractor-operated (COCO) minor application that supports the Bureau of Indian Education's (BIE's) mission by facilitating Indian School Equalization Program (ISEP) transportation reporting by schools, and by calculating allocations based on that reporting in accordance with regulatory requirements established in 25 CFR §§ 39.710 – 39.711, 39.732. WebET 2.0 will enable the agency to distribute ISEP transportation funding timely, fairly, and equitably and will provide for transparency and data analysis.

For schools, WebET 2.0 will be accessible, user-friendly, and comprehensive. For the BIE, WebET 2.0 will be accurate, flexible, and comprehensive, and will enable data analysis and collection of additional data in the event of amendments to current regulation or in response to program needs.

Schools will also use this platform for mandatory reporting of actual transportation cost for reimbursement as required by CFR §§ 39.720-722. This data is reported to Congress and enables analysis and data-based justification for budgetary support.

The WebET 2.0 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?

- 25 C.F.R. Part 39, Subpart G, The Indian School Equalization Program Student Transportation regulations.
- Tribally Controlled Schools Act of 1988, 25 U.S.C. § 2501 *et seq*., as amended by Every Student Succeeds Act of 2015 (ESSA) (Pub. L. 114-95).
- 25 C.F.R. Part 44, regulations for Grants Under the Tribally Controlled Schools Act of 1988.
- Indian Education Amendments of 1978, 25 U.S.C. § 2001 *et seq*., as amended by No Child Left Behind Act, 25 U.S.C. § 2007(a)(1)(B)(ii), Allotment Formula, the need for special staffing, transportation, or educational programs.

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 Bison Governance, Risk, and Compliance (Bison GRC) platform?

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

UII Code: 010-000002901, Web Education Transportation System (WebET 2.0) SSPP

□ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Not Applicable	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)*

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

☒ No

WebET 2.0 is not a Privacy Act system of record as defined at 5 U.S.C. 552a(5).

Information used for the ISEP program may be collected using the Student Transportation Form (OMB Control Number 1076-0134). The information collected on this form is maintained under BIA SORN, INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008), modification publish at 86 FR 50156 (September 7, 2021), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

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

☒ Yes: *Describe*

OMB Control Number 1076-0134, Student Transportation Form, Expires May 31, 2025

□ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: Username, password, user work contact information such as work email, work telephone number, and work address of school staff, such as bus drivers, for account creation purposes; student name and grade when related to air transportation; and bus driver names and salaries, name and signature of the School Principal and Education Line Officer.

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?

PII will be used for WebET 2.0 account management such as sending notifications to users for registration, resetting passwords, issue resolution, resolving late submissions or system issues.

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.*

PII may be shared with BIE employees with a valid "need-to-know" while in the performance of official functions to create accounts and provide program and technical support.

□ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
□ 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 performing services on DOI's behalf as authorized by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Services/EACS), 72 FR 11040 (March 12, 2007), modification published 86 FR 50156 (September 7, 2021), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

□ 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.*

WebET 2.0 users can elect not to provide information during the user account creation process. If an individual declines to provide information or to consent to the specific uses of their PII in WebET 2.0, individual accounts will not be created and access to WebET 2.0 denied.

□ 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.*

Notice is provided through publication of this PIA and the published INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Services/EACS), 72 FR 11040 (March 12, 2007), modification published 86 FR 50156 (September 7, 2021), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

More information about the Department's privacy program including compliance documents and how to submit a request for agency records is available at the DOI Privacy Program website at https://www.doi.gov/privacy-program.

☒ 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 WebET 2.0 are primarily retrieved by school name and school year via a search field.

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 individuals but are produced on transportation mileage. 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; and 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. Driver names and salaries may be used in reports.

□ No

Section 3. Attributes of System Data

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

WebET 2.0 users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is validated by the individual's supervisor during the account creation process.

Data collected using the Student Transportation Form (OMB Control Number 1076-0134) is reviewed by BIE Administrative Officials for accuracy of transportation data submitted to BIE by schools. 25 CFR Part 39, Subpart C – Administrative Procedures, Student Accounts, and Verifications outlines mandatory processes and procedures for ensuring transportation data submitted to WebET 2.0 is accurate. For example, 25 CFR § 39.401 describes accountability of administrative officials by creating procedures that are systematic and can be verified by a random independent outside auditing procedure. These procedures ensure the equitable distribution of funds among schools. 25 CFR § 39.404 describes the certification and verification process each school must follow and the documentation required by subpart G of 25 CFR part 39. 25 CFR § 39.405 states data verifications will be conducted by Education Line Officers.

B. How will data be checked for completeness?

WebET 2.0 users are responsible for ensuring the completeness of the data associated with their user accounts. Data is validated by the individual's supervisor during the account creation process.

Data collected using the Student Transportation Form (OMB Control Number 1076-0134) is reviewed by BIE Administrative Officials for completeness of transportation data submitted to BIE by schools. 25 CFR Part 39, Subpart C – Administrative Procedures, Student Accounts, and Verifications outlines mandatory processes and procedures for ensuring transportation data submitted to WebET 2.0 is complete. For example, 25 CFR § 39.401 describes accountability of administrative officials by creating procedures that are systematic and can be verified by a random independent outside auditing procedure. These procedures ensure the equitable distribution of funds among schools. 25 CFR § 39.404 describes the certification and verification process each school must follow and the documentation required by subpart G of 25 CFR part 39. 25 CFR § 39.405 states data verifications will be conducted by Education Line Officers.

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

WebET 2.0 users are responsible for ensuring the currency of the data associated with their user accounts. Data is validated by the individual's supervisor during the account creation process. Data collected using the Student Transportation Form (OMB Control Number 1076-0134) BIE Administrative Officials for currency of transportation data submitted to BIE by schools. 25 CFR Part 39, Subpart C – Administrative Procedures, Student Accounts, and Verifications outlines mandatory processes and procedures for ensuring transportation data submitted to WebET 2.0 is current. For example, 25 CFR § 39.401 describes accountability of administrative officials by creating procedures that are systematic and can be verified by a random independent outside auditing procedure. These procedures ensure the equitable distribution of funds among schools. 25 CFR § 39.404 describes the certification and verification process each school must follow and the documentation required by subpart G of 25 CFR part 39. 25 CFR § 39.405 states data verifications will be conducted by Education Line Officers.

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

Records are covered by Indian Affairs Records Schedule (IARS) Records Series 5400-Education: School Operations, File Code 5409-P5, Indian School Equalization Program (ISEP) Files and have been scheduled as permanent records by the National Archives and Records Administration (NARA) under Job No. N1-075-05-005, approved October 25, 2005. Records are cut-off at the end of the school year and maintained in the office of record for a maximum of five years. The records are then retired to the American Indian Records Repository (AIRR) which is a Federal Records Center (FRC). Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the United States Department of the Interior (DOI) and the NARA.

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include information technology (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.

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

Data and information maintained within WebET 2.0 is retained under the appropriate NARA approved IARS 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 BIE'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, Departmental policy, and NIST SP 800-88, Guidelines for Media Sanitization.

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

There is a risk to the privacy of individuals due to the PII contained in WebET 2.0. PII in the system is limited to work contact information required to create a user account, usernames, and passwords. WebET 2.0 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. WebET 2.0 is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. 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. BIE manages 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 onboards and until they depart DOI. BSAM is used to establish, activate, modify, review, and disable user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts 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 WebET 2.0 may collect more information that is necessary to complete program goals and objectives. To mitigate this risk the program only collects 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. 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.

WebET 2.0 meets BIE’s information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. WebET 2.0 users are responsible for ensuring the accuracy, completeness, and currency of the data associated with their user accounts. Data is validated by the individual’s supervisor during the account creation process. Data is reviewed by BIE Administrative Officials for accuracy, completeness, and currency of transportation data submitted to BIE by schools. 25 CFR Part 39, Subpart C – Administrative Procedures, Student Accounts, and Verifications outlines mandatory processes and procedures for ensuring transportation data submitted to WebET 2.0 is accurate, complete, and current. For example, 25 CFR § 39.401 describes accountability of administrative officials by creating procedures that are systematic and can be verified by a random independent outside auditing procedure. These procedures ensure the equitable distribution of funds among schools. 25 CFR § 39.404 describes the certification and verification process each school must follow and the documentation required by subpart G of 25 CFR part 39. 25 CFR § 39.405 states, data verifications will be conducted by Education Line Officers.

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 School Operations branch is responsible for managing and disposing of BIE records in WebET 2.0 as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. School Operations branch ensures only records needed to support its program, Tribes, and Tribal members is maintained. The School Operations branch maintains the records for a maximum of five years, at which time they are transferred to AIRR, a FRC for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-05-005, approved October 25, 2005. WebET 2.0 IT records are maintained under DRS 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office’s activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have 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 WebET 2.0 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 adequate notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and the published INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Services/EACS), 72 FR 11040 (March 12, 2007), modification published 86 FR 50156 (September 7, 2021), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices. The PIA and SORN provide a detailed description of system source data elements and how an individual’s PII is used.

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. WebET 2.0 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.

In addition to the risk mitigation actions described above, the BIE maintains an audit trail of activity sufficiently enough to reconstruct security relevant events. The BIE 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 multifactor 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, 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 WebET 2.0 was designed and supports ISEP budget reporting requirements.

☐ 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. WebET 2.0 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: Bureau Operated and Tribal Operated School Administrative personnel provide and have access to transportation data for use with WebET 2.0 system.

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. BIE manages WebET 2.0 user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for ILM. BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards until they depart DOI. BSAM is used to establish, activate, modify, review, disable WebET 2.0 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 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 terms and conditions and the following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

□ No

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

□ Yes. *Explanation*
☒ No

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

☒ Yes. *Explanation*

The purpose of WebET 2.0 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 WebET 2.0 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?

WebET 2.0 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 DOI Rules of Behavior. Users must complete annual IMT Awareness Training, which includes Privacy Awareness, Records Management and Section 508 Compliance training, and 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 WebET 2.0 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*: Multi-Factor Authentication (MFA)

(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 WebET 2.0. 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 WebET 2.0. 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 WebET 2.0 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.