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: Integrated Business Solutions System (IBiS)
Bureau/Office: U.S. Geological Survey (USGS), Office of the Associate Chief Information Officer, Science Information Delivery Branch
Date: November 15, 2022
Point of Contact
Name: Cozenja M. Berry
Title: Associate Privacy Officer
Email: privacy@usgs.gov
Phone: 571-455-2415
Address: 12201 Sunrise Valley Drive, Mail Stop 159, Reston, VA 20192

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

B. What is the purpose of the system?

The Integrated Business Solutions (IBiS) system is a centralized point of sales system utilized by the U.S. Geological Survey (USGS) Store. The USGS Store is a component of the Science Information Delivery Branch (SID), Office of the Associate Chief Information Officer (OACIO), USGS. Through partnerships with the National Park Service (NPS), the Bureau of Land Management (BLM), the United States Fish and Wildlife Service (FWS), the United States

Forest Service, and other federal agencies, the USGS Store offers recreational lands passes, earth science products, and forestry products to the general public. Products available for purchase or issuance through the store include: America the Beautiful - The National Parks and Federal Recreational Lands Pass; government produced maps; satellite imagery prints; science publications; and a variety of educational materials. IBiS only collects information that is necessary to execute the responsibilities associated with the sale or issuance of products and to respond to inquiries received by the USGS Store.

All USGS Store customers must provide their name, mailing address, email address and phone number when creating a customer account. Credit card information (to include billing address) is only collected when orders require a form of payment. As an additional data protection measure, customer information is stored in separate tables from payment information. Credit card data is encrypted on entry and can only be unencrypted by USGS personnel with accounting permissions. IBiS does not save or retain credit card information for future orders. All payments are processed securely utilizing Pay.gov, a service of the U.S. Department of the Treasury, Bureau of the Fiscal Service. The privacy policies for Pay.gov may be reviewed at https://www.pay.gov/public/home/privacy and the Privacy Impact Assessment (PIA) may be reviewed at https://fiscal.treasury.gov/files/pia/paygov-pclia.pdf.

Customers requesting discounted or free recreational lands passes (Senior pass, Access pass, Military pass) must provide identification or documentation that reflects date of birth, citizenship, disability, or military service as required for proof of eligibility. The USGS may share this personal data with a third-party vendor to assist with verifying eligibility. For orders requiring special print service, the customer's name, shipping address, and product order information may be shared with a third-party vendor to complete order fulfillment. Federal Acquisition Regulation (FAR) clauses requiring compliance with the Privacy Act of 1974 are included in contracts for third-party vendors providing such services. Customer data shared by the USGS may only be used for the purposes described herein and as specified in the contract. Further, third party vendors are not authorized to sell, share, or otherwise propagate customer data provided by the USGS.

The USGS also uses IBiS to support fulfillment of recreational lands passes ordered through Recreation.gov (rec.gov). Rec.gov is a cloud-based Software as a Service (SaaS) travel planning system managed by the USDA Forest Service by the Director of Recreation, Heritage and Volunteer Resources. The USGS Store receives name and shipping address only from Rec.gov to ship passes to customers who order through Rec.gov. No payment information or other PII is exchanged between Rec.gov and IBiS. On fulfillment of orders, the USGS provides USDA with shipping information for their customer records. The USDA PIA for rec.gov may be viewed at https://www.usda.gov/sites/default/files/documents/nre-fs-r1s-pia.pdf.

Security controls applied to IBiS include user identification, multi-factor authentication, encryption, firewalls, audit logs, network system security monitoring, and software controls. To prevent unauthorized access, IBiS is managed by use of role-based permissions. In addition, USGS employees and contractors must complete privacy, security, and records management

awareness training, as well as annual role-based refresher training. System users must also sign rules of behavior which prescribes additional practices and security controls specific to IBiS.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 7 U.S.C. 1387, Photographic reproductions and maps; 16 U.S.C. 6804, Recreation passes; 31 U.S.C. 9701: Fees and charges for Government services and things of value; 43 U.S.C. 1457: Duties of Secretary; 43 U.S.C. 31, Director of United States Geological Survey; 43 U.S.C 31c, Geologic mapping program; 43 U.S.C. 41, Publications and reports; preparation and sale; 43 U.S.C. 42, Distribution of maps and atlases, etc.; 43 U.S.C. 42a, Use of receipts from sale of maps for map printing and distribution; 43 U.S.C. 43, Copies to Senators, Representatives, and Delegates; 43 U.S.C. 44, Sale of transfers or copies of data; 43 U.S.C. 45, Production and sale of copies of photographs and records; disposition of receipts; 7 CFR 2.60, Chief, Forest Service.

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: 010-000002291, System Security and Privacy Plan for Asset 442 Integrated Business Solutions System

☐ 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	------	------	------

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

☒ Yes.

Records pertaining to the sale of recreational lands passes are maintained under INTERIOR/DOI-06, The America the Beautiful--The National Parks and Federal Recreational Lands Pass System, 80 FR 63246 (October 19, 2015); modification published at 86 FR 50156 (September 7, 2021).

Records pertaining to the sale of earth science and forestry products (government produced maps, satellite imagery prints, science publications, and educational materials) are maintained under INTERIOR/USGS-15, Earth Science Information Customer Records, 63 FR 60374 (September 11, 1998); modification published at 74 FR 23430 (May 19, 2009). **Note:** Due to significant changes to the scope of records covered under INTERIOR/USGS-15, the USGS is proposing to issue a new SORN, INTERIOR/USGS-28, U. S. Geological Survey (USGS) Store Customer Records. A rescindment notice will be issued for INTERIOR/USGS-15 after publication of INTERIOR/USGS-28 in the Federal Register and conclusion of the public comment period.

Published notices may be viewed on the DOI Privacy website at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes. OMB Control 1024-0252 for the America the Beautiful: The National Parks and Federal Recreational Lands Pass applications. The latest approval expires 9/30/2023 and can reviewed at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202006-1024-007.

Note: The IBiS information collections related to earth science and forestry product transactions do not require an OMB Control number as they are categorized as voluntary commercial sales orders.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Birth Date
☒ Disability Information
☒ Credit Card Number

☒ Driver's License
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: Individuals are automatically assigned a unique Customer ID number that can be used to sign in their account (email address may also be used for sign in). A password is also required on account creation. Customers may choose to use their business or other organizational information in lieu of personal information when establishing a customer account with the USGS Store.

Only customers requesting discounted or free recreational lands passes (Senior pass, Access pass, Military pass) must provide an acceptable identification (such as a U.S. Driver's License, Green Card, or U.S. Passport) or other documentation to verify date of birth, citizenship, disability, or military service as required for proof of eligibility. Customers may provide documentation that includes other PII elements or personal information when submitting proof of eligibility for discounted or free recreational lands passes. Information that is not required for processing these orders is destroyed and not retained by the USGS.

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*

PII is collected directly from individuals who patronize the USGS Store. Additionally, the USGS receives customer information (name and shipping address) from the USDA Forest Service to process orders for recreational lands passes purchased from Rec.gov.

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. Pass orders may also be received from Recreation.gov (rec.gov). Rec.gov is a travel planning system managed by the USDA Forest Service. USGS receives name and shipping address only from Rec.gov to ship recreational lands passes to customers who order through Rec.gov. No other PII is exchanged between Rec.gov and IBiS. The USDA PIA for rec.gov may be viewed at https://www.usda.gov/sites/default/files/documents/nre-fs-r1s-pia.pdf.

☐ Other:

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

Personal information is collected in IBiS to complete sales and distribution of products from the USGS Store and to respond to customer inquiries. Customer names, contact information, shipping addresses, and payment information are needed to complete sales transactions. Government issued identification, proof of military service, and proof of disability are collected from individuals to verify eligibility for discounted or free recreational lands passes (Senior pass, Military pass, Access pass). Deidentified data may be used to report trends to partner agencies in research for possible future distribution opportunities.

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

☒ Within the Bureau/Office: Personal information collected in IBiS is only used for the intended purposes as stated above. Access to customer account information is restricted to USGS government employees and contractors in the Science Information Delivery (SID) Branch who perform duties supporting the USGS Store.

☒ Other Bureaus/Offices: PII is not routinely shared with other bureaus and offices. It is permissible to share PII from IBiS with authorized DOI personnel who have a need-to-know in the performance of their official duties.

☒ Other Federal Agencies: PII may be shared with the Treasury Department through the use of Pay.gov to process credit card transactions.

PII is not routinely shared from IBiS to other Federal agencies. It is permissible to disclose records to Federal law enforcement authorities when, either alone or in conjunction with other information, indicates a violation or potential violation of law (criminal, civil, or regulatory in nature).

☒ Tribal, State or Local Agencies: PII is not routinely shared from IBiS to Tribal, State or Local Agencies. It is permissible to disclose records to any criminal, civil, or regulatory law enforcement authority when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law (criminal, civil, or regulatory in nature).

☒ Contractor: Eligibility documents may be shared with contractors to verify customer eligibility for discounted or free passes. The contractor uses select data points to verify eligibility for the pass and then deletes the data. Orders that require map printing are sent to a third party vendor with the customer's name and address for order fulfillment and shipping. Lastly contractors directly supporting the USGS Store may perform tasks involving customer service, order fulfillment, and system administration for the IBiS application and infrastructure. The required Federal Acquisition Regulation (FAR) clauses for compliance with the Privacy Act of 1974 (as amended) are included in contracts.

☒ Other Third Party Sources: PII is not routinely shared from IBiS with third parties. Additional disclosures may be permitted only when consistent with the purpose of the activity and the uses authorized under the Privacy Act and as stated in the routine uses in INTERIOR/ USGS-15, Earth Science Information Customer Records and INTERIOR/DOI-06, The America the Beautiful--The National Parks and Federal Recreational Lands Pass System.

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

☒ Yes: As this is an e-commerce site, customers must create an account before making a purchase. All requested PII is optional, however if the customer declines to provide the information, the USGS Store will be unable to provide the product(s) to the customer. The USGS makes some of its earth science and educational products available as free downloads; customers are not required to establish an account to access free downloads.

☐ No:

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

☒ Privacy Act Statement:

The following Privacy Act Statement is posted on the USGS Store login screen and is available to all users who access the system.

Privacy Act Statement
Authority: 5 U.S.C. 301; 7 U.S.C 1387; 16 U.S.C. 6804; 31 U.S.C. 9701; 43 U.S.C. 1457; 43 U.S.C. 31; 43 U.S.C 31c; 43 U.S.C. 41; 7 CFR 2.60, Chief, Forest Service.

Purpose: Information is collected to complete sales and distribution of products from the USGS Store. Customer names, contact information, shipping addresses, and payment information are needed to complete sales transactions. Government issued identification, proof of military service, and proof of disability may be collected from individuals to verify eligibility for discounted or free recreational lands passes (Senior pass, Military pass, Access pass).

Routine Uses: Information may be disclosed to DOI officials and its contractors to facilitate distribution of purchased maps, America the Beautiful - The National Parks and Federal Recreational Lands Pass, government produced maps, satellite imagery prints, science publications, and educational materials. In addition, information may be disclosed to other organizations as authorized under the Privacy Act or outlined in the routine uses in INTERIOR/ USGS-15, Earth Science Information Customer Records (63 FR 60374); INTERIOR/DOI-06, The America the Beautiful--The National Parks and Federal Recreational Lands Pass System (80 FR 63246) which may be viewed at https://www.doi.gov/privacy/sorn.

Disclosure: Providing this information is voluntary. Individuals do not have to provide their personal information but not doing so may limit one's ability to purchase products from the USGS Store.

☒ Privacy Notice: The customer has access to the information provided in the following link, which details information on the Privacy Act: https://www.usgs.gov/privacy-policies.

☒ Other: The associated system of records notices and this assessment also serve to notify as public notification for the collection and use of personal information in IBiS.

☐ None

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

IBiS uses a unique customer number to identify a customer master record, which contains the address, billing information, email, phone number and product and financial data related to orders in the system. The customer number is the primary identifier used to retrieve customer records. Records may also be retrieved by last name/first name, email address, address attributes, phone number, a purchase order number, or by company name.

I. Will reports be produced on individuals?

☒ Yes: Reports are generated on individuals to fulfill orders and to troubleshoot incomplete orders. Customer reports only reflect customer number, name, shipping address, and products ordered. Only users assigned permissions to create reports via an administrative role can create them. Reports may be shared with third party vendors who are contracted to fulfill map request that require special printing services. These reports are temporary and destroyed after their intended use.

☐ No

Section 3. Attributes of System Data

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

Customers have the responsibility to verify the accuracy of their PII data entries. The customer gets multiple prompts to verify the data is correct in the form of reviewing the order, receiving email notification of order confirmation and shipping confirmation email. If at any time they find a discrepancy, they may contact the USGS Store call center who will update the account with the correct information as well as correct any orders that may be in process.

Customer records for recreational lands passes that are received from the USDA Forest Service through Rec.gov are presumed to be accurate. The data fields in IBiS are coded to validate the entry based on data type and format. Certain fields are mandatory for completion and users are prompted at various points to review data for accurate input. Rec.gov verification procedures are described in the Rec.gov PIA available at https://www.usda.gov/sites/default/files/documents/nre-fs-r1s-pia.pdf.

B. How will data be checked for completeness?

Customers have the responsibility to verify their data entries are complete. The customer account and credit card payment forms have mandatory fields that must be filled in to complete these processes. In addition, for the Senior pass, Access pass, and Military pass purchases, customers are required to submit documents to verify eligibility for discounted or free passes. If the documents submitted do not have the necessary information, the USGS Store will contact the customer via phone, email, or mail to request the necessary information.

Customer records shared with the USGS by the USDA Forest Service through Rec.gov are presumed to be complete. Discrepancies identified by the USGS Store when processing Rec.gov orders are referred back to Rec.gov for verification and correction of the record.

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

To create an account the customer must provide the required data. Customers can also update their account information at any time. This information is provided on the USGS Store site and documented in USGS Store internal business procedures.

Rec.gov is responsible for ensuring customer data shared with IBiS is current. Discrepancies identified by the USGS Store when processing Rec.gov orders are referred back to Rec.gov for verification and correction of the record.

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

Data are retained in accordance with the USGS General Records Disposition Schedule (GRDS). The applicable GRDS is 305-06, IBiS System, which supports the distribution of USGS published materials such as maps, books, and scientific reports in addition to products from other

Federal agencies. These records have a temporary disposition and cut-off at the end of the fiscal year in which files are closed. Records in IBiS are retained for 6 years and 3 months.

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

Paper records are shredded in accordance with records retention guidelines. Electronic records are deleted. Backup tapes are reinitialized and reused. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy, and National Archives and Records Administration (NARA) guidelines.

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 are risks to the privacy of individuals due to the volume of sensitive PII contained in IBiS. This risk is mitigated through administrative, physical, and technical controls that have been implemented to protect the confidentiality, integrity, and availability of information in the system. IBiS 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, disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit card information, and exposure of sensitive information.

The collection of documentation required to prove eligibility for discounted or free recreational lands passes poses a privacy risk to individuals if compromised. Only customers requesting discounted or free recreational lands passes (Senior pass, Access pass, Military pass) must provide an acceptable identification (such as a U.S. Driver's License, Green Card, or U.S. Passport) or other documentation to verify date of birth, citizenship, disability, or military service as required for proof of eligibility. There is a risk that users may submit more information than is necessary for the verification process. This risk is mitigated by USGS specifying the information necessary for customers to demonstrate eligibility. Further to minimize the collection of PII, USGS Store customer policy states that the DD 214, *Certificate of Release or Discharge from Active Duty* should not be submitted as proof of military service. Only relevant data is retained to complete the verification process; extraneous documentation submitted by customers is destroyed on receipt. Orders for recreational lands passes that are received by mail are scanned and encrypted; after verifying the image capture is good, the paper copy is shredded by USGS Store personnel.

The collection of payment information to purchase products poses a risk for fraudulent activities. For all orders requiring a payment, credit card data is automatically encrypted on entry to IBiS and can only be unencrypted by the accounting team. All payments are processed securely utilizing Pay.gov, a service of the U.S. Department of the Treasury, Bureau of the Fiscal Service. The privacy policies for Pay.gov may be reviewed at https://www.pay.gov/public/home/privacy and the PIA may be reviewed at https://fiscal.treasury.gov/files/pia/paygov-pclia.pdf.

Data minimization is also enforced with orders for recreational lands passes that are received from and fulfilled on behalf of USDA via Rec.gov. The USGS only receives customer name, shipping address, number and type of pass(es) requested from Rec.gov. No payment information or other PII is collected or maintained in IBiS from Rec.gov. USGS only serves as a distribution point, all customer communications related to these records are handled by USDA personnel. The USDA PIA for rec.gov may be viewed at https://www.usda.gov/sites/default/files/documents/nre-fs-r1s-pia.pdf.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. To mitigate this risk, the USGS Store follows the least privilege security principle and strictly limits access to customer data based on an official need to know. Additionally, customer data is only used for the purposes as specified in this privacy impact assessment and in the associated system of records notices. Customer data may be shared with contractors to verify eligibility for discounted and free recreational lands passes, and to fulfill map orders that require special printing services. Customer information shared with contractors is limited to only the data necessary to process the request (name, address, email address, and product ordered). Further, these vendors are not authorized to use, sell, share, or otherwise propagate customer data provided by the USGS. Access to records in the IBiS is limited to authorized personnel who have a need to access the records in the performance of their official duties. Further, each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols. All users must complete records management, Paperwork Reduction Act (PRA), Section 508, Controlled Unclassified Information (CUI) and role based security and privacy training on an annual basis. Moreover, they must review and agree to the DOI Rules of Behavior.

There is a risk that information in the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The IBiS system owner will ensure that the identified records are maintained and disposed of in accordance with records retention schedules that were approved by NARA. IBiS users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Customer records regardless of media (paper or electronic) are closely safeguarded in accordance with applicable laws, rules and policies.

There is a risk that individuals may not receive adequate notice of the purposes for collecting their personal information in IBiS or whom the information may be shared with. Individuals are notified of the privacy practices through published DOI SORNs, Privacy Act Statement, and the USGS website Privacy Policy. This PIA also provides a detailed description of IBiS data elements, uses of personal information, and how customer PII is shared.

Security controls have been implemented to prevent unauthorized access to customer data throughout the information lifecycle. The IBiS employs Transport Layer Security (TLS) technology to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Audit Logs are kept on all system activity with tools in place to look for abnormal activity and intrusion

detection. Other system security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection tools.

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: The purpose for collecting personal information in IBiS is to fulfill orders and respond to customer inquiries. Customers requesting discounted or free recreational lands passes (Senior pass, Access pass, Military pass) are required to provide identification or documentation to prove eligibility.

☐ No

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

☐ Yes

☒ No. Information only as it pertains to the order fulfillment (confirmation, processing, shipping) and notes related to customer inquiries and interactions may be updated in individual records.

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?

N/A. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

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*

USGS employees and contractors (users) must have a DOI Active Directory account assigned by their bureau or office and have need-to-know in order to perform their official duties. The system may only be accessed from within the DOI network or using the DOI Virtual Private Network (VPN). All users must authenticate using a PIV card issued by DOI.

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

Access to IBiS for USGS employees and contractors (users) is determined by functional responsibilities. Users must complete both a User Certification Form and system authorization access request, which must be signed by their supervisor. Access control lists are used to manage access to the data. System Administers work with supervisors to define user roles, change permissions, and remove access as needed. USGS Store customer access is restricted to their own account registration information and order history. Customers do not have access to other individuals PII or account information.

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. Privacy Act contract clauses are included in all contracts. Contractors must sign a non-disclosure agreement upon employment and are required to complete annual privacy and information security training.

☐ 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. User monitoring is limited to information provided in system and web logs for system security administration purposes only.

☐ No

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

IT audit logs include username, hostname, logon dates, times of failed logon attempts, IP addresses, webpages accessed, processes accessed and other system failures.

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

The USGS complies with the National Institute of Standards and Technology and other Federal requirements for data security as part of a formal program of Assessment and Authorization, and continuous monitoring. Periodic scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any equipment. The use of USGS IT systems is conducted in accordance with the appropriate use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security-relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis, and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Access to administrative functions is strictly controlled. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource. USGS personnel with system administrator access must complete IT security and privacy awareness training as well as role-based training before being granted access to the system, when required by system changes, and at least annually thereafter.

Access to IBiS for USGS employees and contractors (users) is determined by functional responsibilities. Users consent to monitoring when accessing government maintained systems. In addition, use of personally owned equipment is prohibited; government furnished equipment must be used to access the system. IBiS users are required to complete a system authorization access request, which must be signed by their supervisor.

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 Chief, Science Information Delivery Branch is the IBiS System Owner and the official responsible for oversight and management of IBiS security and privacy controls, including the

protection of information processed and stored by IBiS. The System Owner is also designated as the Privacy Act system manager and is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, 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 USGS Associate Privacy Officer (APO). Specific guidance on how DOI implements the Privacy Act has been published to the Code of Federal Regulations at 43 CFR Part 2, Subpart K.

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 IBiS System Owner is responsible for oversight and management of the system security and privacy controls and for ensuring, to the greatest possible extent, that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team and DOI Computer Incident Response Center immediately upon discovery in accordance with Federal policy and established procedures. Incidents involving PII must be reported to the USGS APO and are managed in accordance with procedures outlined in the DOI Privacy Breach Response Plan. The APO oversees breach reporting and response activities to include incident investigation, mitigation efforts, and implementing corrective actions following a breach.