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: U.S. Geological Survey - Infrastructure
Bureau/Office: U.S. Geological Survey/Office of Enterprise Information
Date: February 15, 2019
Point of Contact:
Name: Alan Wiser
Title: Associate Privacy Officer (Acting)
Email: awiser@usgs.gov
Phone: (865) 322-0241
Address: 12201 Sunrise Valley Drive, 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: *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 purpose of the U.S. Geological Survey (USGS) Infrastructure (INFRA) system is to provide a USGS-wide collaborative environment for information storage, sharing, and processing among offices, programs, science centers, and their collaborators. The USGS relies on INFRA to provide a single infrastructure for cross-organization communication and collaboration, thus reducing unnecessary time, resources, and costs spent on supporting disparate or outdated tools. Due to the nature of INFRA, users may store all types of electronic files including text, graphical, audio, or visual files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of personally identifiable information (PII) may be included in the documents stored in INFRA. INFRA has the following components:

USGS SharePoint
USGS SharePoint provides a secure collaborative workspace and a set of tools where users can store and manage documents and calendars, compile information, manage lists and discussion databases, and do other tasks to conduct and manage projects across time zones and networks with science partners inside and outside the USGS. WebForms are standardized forms in USGS SharePoint that are used bureau-wide for specific mission purposes.

National Web Server System (NatWeb)
USGS NatWeb provides secure, reliable, and high-availability web hosting solutions for USGS offices and programs. NatWeb websites are segregated into two categories, USGS-only access and public access.

Hosting Platform Hardware (HPH)
USGS HPH provides an “Infrastructure as a Service” (IaaS) platform providing virtualized servers and data storage for USGS programs and offices.

Enterprise File Transport Protocol (eFTP)
USGS eFTP provides the ability to transfer digital files between USGS science centers and non-USGS science collaborators.

USGS Listserver
The USGS Listserver is a mailing list server running a software program for handling email list subscription requests and distributing email messages to list subscribers worldwide. The USGS Listserver only allows list “owners” to distribute messages to list subscribers. A list owner is a USGS employee who has authority (e.g., from a supervisor) to distribute messages to specific email lists.

C. What is the legal authority?

5 U.S.C. 301, 3101, 5105–5115, 5501– 5516, 5701–5709; 31 U.S.C. 66a, 240– 243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Executive Order 11807; 40 U.S.C. 486(c); 41 CFR part 201-7.

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*

010-000001010; System Security Plan (SSP) for Infrastructure

☐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.*
Hosting Platform Hardware (HPH)	HPH consists solely of hardware and VMware for hosting virtualized operating systems	No	N/A

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)*

Due to the nature of INFRA, which helps the USGS collaborate, create, and process records in support of specific mission purposes, there are many applicable System of Records Notices (SORNs), but the two listed are representative of records that are generally contained in INFRA:

DOI-58, Employee Administrative Records, 64 FR 19384, April 20, 1999, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-1999-04-20/pdf/99-9830.pdf. A new routine use was added on February 13, 2008, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2008-02-13/pdf/E8-2584.pdf.

USGS-18, Computer Registration System, 63 FR 60376, November 9, 1998, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-1998-11-09/pdf/98-29910.pdf. A new routine use was added on May 19, 2009, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2009-05-19/pdf/E9-11613.pdf.

☐No

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

☐Yes: *Describe*
☒No

Section 2. Summary of System Data

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

☒Name
☒Citizenship
☒Gender
☒Birth Date
☒Group Affiliation
☒Marital Status
☒Biometrics
☒Other Names Used
☒Truncated SSN
☒Legal Status
☒Place of Birth
☒Religious Preference
☒Security Clearance
☒Spouse Information
☒Financial Information
☒Medical Information
☒Disability Information

☒Credit Card Number
☒Law Enforcement
☒Education Information
☒Emergency Contact
☒Driver's License
☒Race/Ethnicity
☒Social Security Number (SSN)
☒Personal Cell Telephone Number
☒Tribal or Other ID Number
☒Personal Email Address
☒Mother's Maiden Name
☒Home Telephone Number
☒Child or Dependent Information
☒Employment Information
☒Military Status/Service
☒Mailing/Home Address

☒Other: *Specify the PII collected.* Internet Protocol (IP) Address

All these types of PII may potentially be included by users of these services. The USGS Listserver contains name and personal email address. This information is manually entered by the list subscriber. Due to the nature of USGS SharePoint, users may store all types of electronic files including text, graphical, audio, or visual files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in USGS SharePoint. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers, dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose.

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* INFRA may contain PII of collaborators as the USGS collaborates with many stakeholders across state and local agencies.

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: *Describe*

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

PII is used to control access to INFRA by system administrators. Email addresses are sent to the USGS Listserver for sending email messages to list subscribers. USGS SharePoint provides a storage and collaborative environment for USGS personnel and offices to interact with each other within the USGS. PII may be used for a variety of purposes within USGS SharePoint at the local level by specific programs in support of a specific mission purpose. Due to the purpose of INFRA and the range of supported services in USGS SharePoint, personal information may be present for a variety of reasons as part of the function of the program office during communication, collaboration, and creation and management of records.

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.*

Data is shared by system administrators to grant and manage access to the services and contents stored within INFRA for collaboration purposes. System administrators have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions. Each user of the service will have access to their own data within the system and will be able to access other contents based on rights granted.

☐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.*

Other Federal agencies do not have access to the system or any services within the system. However, data may be shared with other Federal agencies as necessary to meet legal or mission requirements, or in the course of conducting official business. For example, exchange of communications or correspondence generated from use of the services. Information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in the DOI-58: "Employee Administrative Records" and USGS-18: "Computer Registration System" SORNs.

☒Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Tribal, state or local agencies do not have direct access to the system or any services within the system. Data may be shared with Tribal, state or local agencies as necessary to meet legal or mission requirements, or in the course of conducting official business.

☒Contractor: *Describe the contractor and how the data will be used.*

Microsoft is a Cloud Service Provider that will provide vendor support for the USGS SharePoint environment. Per contractual obligations, they have no authorization to review, audit, transmit, or store USGS data. The USGS may have contractor support within program areas, and these contractors will have limited access to contents of the services in the system. Information may be shared with contractors who perform services or otherwise support USGS activities related to INFRA, and as authorized pursuant to the routine uses contained in the DOI-58: "Employee Administrative Records" and USGS-18: "Computer Registration System" SORNs.

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

Third-party organizations do not have direct access to the system or any services within the system. Data may be manually shared with other third parties as authorized and necessary to meet legal or mission requirements, or in the course of conducting official business. Information may be shared with other third-party sources as authorized pursuant to the routine uses contained in the DOI-58: "Employee Administrative Records" and USGS-18: "Computer Registration System" SORNs.

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 is voluntarily provided in USGS SharePoint based on the program office's needs in fulfilling its business functions. Subscribing to a USGS-owned email list through the USGS Listserver is optional as well, and an opt-out capability is provided once subscribed.

☐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.*

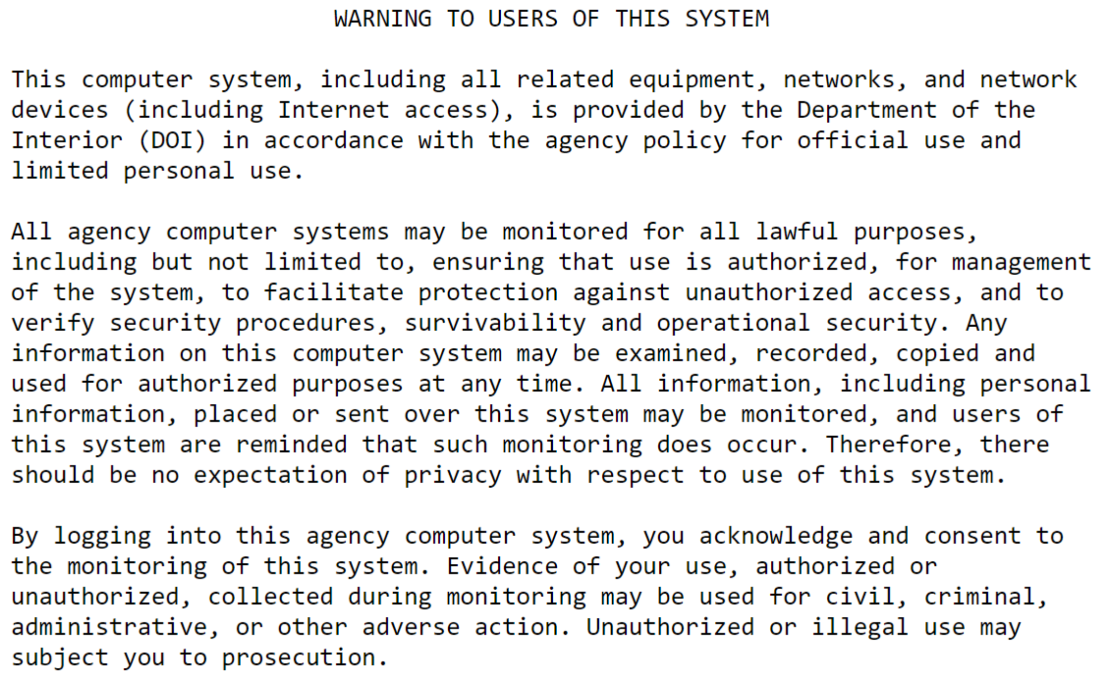
For Privacy Act systems in USGS SharePoint, a Privacy Act Statement is provided at the point of collection on WebForms. For non-WebForms, it is the responsibility of each user, in consultation with the USGS Privacy Program, to provide a Privacy Act Statement for any collections requesting PII.

USGS Listserver Privacy Act Statement

Furnishing the requested information is voluntary. You are not required to provide your name. You must provide your email address to receive email messages from the USGS Listserver. The information you provide is used only for sending email messages to email list subscribers. The information requested is authorized by 40 U.S.C. 486(c) and 41 CFR part 201–7. The records for this collection will be maintained in the appropriate Privacy Act system of records identified as Computer Registration System–Interior, USGS-18 (63 FR 60376), which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-1998-11-09/pdf/98-29910.pdf. A new routine use was added to this System of Records Notice on May 19, 2009, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2009-05-19/pdf/E9-11613.pdf.

☒Privacy Notice: *Describe each applicable format.*

Privacy Notice is provided to individuals through the publication of this Privacy Impact Assessment. In addition, the following warning banner is provided to all users logging in to a USGS computer system:



```
                         WARNING TO USERS OF THIS SYSTEM

This computer system, including all related equipment, networks, and network
devices (including Internet access), is provided by the Department of the
Interior (DOI) in accordance with the agency policy for official use and
limited personal use.

All agency computer systems may be monitored for all lawful purposes,
including but not limited to, ensuring that use is authorized, for management
of the system, to facilitate protection against unauthorized access, and to
verify security procedures, survivability and operational security. Any
information on this computer system may be examined, recorded, copied and
used for authorized purposes at any time. All information, including personal
information, placed or sent over this system may be monitored, and users of
this system are reminded that such monitoring does occur. Therefore, there
should be no expectation of privacy with respect to use of this system.

By logging into this agency computer system, you acknowledge and consent to
the monitoring of this system. Evidence of your use, authorized or
unauthorized, collected during monitoring may be used for civil, criminal,
administrative, or other adverse action. Unauthorized or illegal use may
subject you to prosecution.
```

☐Other: *Describe each applicable format.*

☐None

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

Data from the USGS Listserver is retrieved by email address and possibly first name and last name, if furnished by the subscriber. Data is retrieved from USGS SharePoint by any defined field within the record. These fields may include, but are not limited to, name, work email address, work phone number, and office location.

I. Will reports be produced on individuals?

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

☒No

Section 3. Attributes of System Data

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

INFRA contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of each user to ensure accuracy of data at the time the data is created or used. System administrators ensure user information is accurate through user request forms submitted by the user and through authentication with the Active Directory (AD) service, and will not ensure accuracy of specific data created or entered by end users.

B. How will data be checked for completeness?

INFRA contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of each user to ensure completeness of data. USGS SharePoint and USGS Listserver data owners are responsible for verifying and updating the information relevant to their use of the services. Upon request from the users, the users' specific account attributes can be updated. System administrators ensure completeness of user information for access control and authentication with the AD service, and will not ensure data created or entered by end users is complete.

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

INFRA contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services, it is the responsibility of each user to ensure currency of the data created or used. Data that is auto-generated in WebForms is pulled from the AD service and can be updated by contacting the USGS Service Desk. AD is updated immediately upon a change in an employee's status, which will automatically update access to INFRA as only active and authorized employees will have access. When a user account is disabled or terminated, all access will be denied since the user will no longer have the ability to log onto or authenticate to the system. USGS Listserver data is updated by the administrator, who removes duplicate email subscriptions upon visual inspection of the subscription lists. Within the organization, users have the ability to enter their own information and to ensure that it 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.

Retention records vary depending on the user-created or user-managed contents and purpose of the program records. Records contained within INFRA are retained and disposed of in accordance with the USGS General Records Disposition Schedule (GRDS), approved by the

National Archives and Records Administration (NARA) for each type of record based on the subject or function and records series.

Electronic records within INFRA that used for audit logging are maintained in accordance with the USGS GRDS, Item 210-01 – Files and Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records. Records are deleted or destroyed when one year old or when no longer needed for administrative, legal, audit, or other operational purposes, whichever is later.

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 or pulped 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, Department of the Interior (DOI) records policy, and 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 is a privacy risk to individuals due to the potentially large amounts of PII contained in INFRA, particularly within USGS SharePoint. Mitigating controls are implemented to protect data. INFRA-authorized end users are allowed to edit or view the documents based on their authorized subsystem roles and the specific job functions. System, network, application, and database level access is controlled strictly on a need-to-know basis. Appropriate background investigations are conducted before any access is granted. No anonymous access is allowed. All system activities are logged and constantly monitored. All employees and contractors with access to the system must go through an annual IT security awareness and privacy awareness training. Appropriate warning banners are displayed at the login time. All system users must acknowledge and follow the rules of behavior as prescribed in the system rules of behavior.

INFRA has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. INFRA is rated as FISMA moderate based upon the type of data contained, and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII contained in the system. INFRA has developed a System Security Plan based on NIST guidance and is part of a Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on INFRA to identify and mitigate any found vulnerabilities. Security and privacy awareness training is required for all USGS employees and information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter. All users must sign the DOI Rules of Behavior. Security role-based training is also required for security personnel and officials with special roles and privileges.

The USGS complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. 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.

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*

Data stored within USGS SharePoint is relevant and necessary to process information in WebForms, or to facilitate storage and sharing of information among offices, programs, science centers, and their collaborators. Data collected for the USGS Listserver is necessary to send email messages to subscribers.

☐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. INFRA 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. *Describe the controls that are in place to protect the data from unauthorized access or use.*

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

☒No, data or processes are not being consolidated.

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

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

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

Access is controlled through user account management and authentication with AD. Access will be obtained only by those whose names are on the access control lists of the system. Access to the data is determined by an individual's "need-to-know," job description, and decision of the program office managing the application. Criteria, procedures, controls, and responsibilities regarding access are documented by those responsible for the data. NatWeb content administrators determine access rights on a site-by-site basis. The USGS Listserver is configured so that only list owners can view subscriber lists to the lists in which they own. The USGS

Listserver administrator can view all subscriber lists to perform routine administrative functions, such as removing an email address from a subscriber list.

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?*

Privacy Act contract clauses are included in contracts.

☐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*

INFRA uses audit logs to record access to the system, and access to the data. Logon date and time, IP address, logoff data and time, and process accessed are recorded in system audit logs. Logs are reviewed daily.

☐No

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

INFRA is not intended to be used to monitor individuals. USGS SharePoint provides audit capabilities on addition, modification, or deletion of data within the system. This information is only available to administrative personnel. Administrator reviews will also help prevent any unauthorized monitoring or user behaviors. IP address, logon and logoff time, and processes accessed are recorded in audit log files.

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

The USGS complies with NIST and other Federal requirements for data security as part of a formal program of Assessment and Authorization, and continuous monitoring. Monthly 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 INFRA 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. Users 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. All users must sign the DOI Rules of Behavior.

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 INFRA System Owner serves as the Information System Owner and the official responsible for oversight and management of INFRA’s security and privacy controls, including the protection of information processed and stored by INFRA. The Information System Owner and Information System Security Officer 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 by INFRA. The System Manager 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 Associate Privacy Officer.

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 INFRA Information System Owner is responsible for oversight and management of the INFRA security and privacy controls and for ensuring, to the greatest possible extent, that INFRA agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information 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 immediately upon discovery in accordance with Federal policy and established procedures.