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: Geospatial Platform (GeoPlatform)
Bureau/Office: Office of the Chief Information Officer
Date: June 16, 2022
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

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 Geospatial Platform (GeoPlatform) is a long-term, high-level project to drive cloud adoption of geospatial applications and data for federal agencies that is managed by the Department of the Interior (DOI), a partner of the Federal Geographic Data Committee (FGDC) that is comprised of agency members responsible for the National Geospatial Data Asset (NGDA) Themes as designated in OMB Circular A-16, *Coordination of Geographic Information and Related Spatial*

Data Activities, Appendix E. The GeoPlatform offers access to a suite of geospatial resources including data, services, and applications through an online portal called GeoPlatform.gov and Federal Risk and Authorization Management Program FedRAMP, Geospatial Information System (GIS) cloud hosting services (CHS) through Amazon Web Services (AWS) East/West. The intent of GeoPlaform's CHS is to reduce costs while improving efficiency for geospatial information sharing and allowing multiple agencies and partners to leverage shared services in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 500-292 and NIST SP 800-53. GeoPlatform.gov is hosted in a Platform-as-a-Service (PaaS) environment through GeoPlatform GIS CHS and maximizes geospatial interoperability by making Federal geospatial data Findable, Accessible, Interoperable, and Reusable (FAIR), and available in various open standard formats. This strategic national resource supports the Federal Administration's Open Government, Open Data, and Digital Government strategies that enhance transparency, collaboration, and participation.

The GeoPlatform is a key component connecting many goals of the National Spatial Data Infrastructure (NSDI) Strategic Plan, including advancing the NSDI. The portfolio of data services, applications and tools, and shared services provided on GeoPlatform.gov is stewarded through the use of open licenses and careful review. GeoPlatform.gov also provides streamlined access to NGDAs and reduces data duplication. The collaborative GeoPlatform Marketplace provides a listing of datasets that one or more member agencies of the FGDC are planning for acquisition to help reduce data acquisition costs. The GeoPlatform's tools, system reports, and dashboards support the OMB Circular A-16 portfolio management process. These services are managed in accordance with OMB Circular A-16, Executive Order 12906, Cloud First Policy, Data Center Optimization Initiative (DCOI), E-Government Act of 2002, and the Geospatial Data Act of 2018. Both offerings are available to the member agencies of the FGDC and their partners at the Federal, State, Tribal, and Local government levels. The GeoPlatform also offers GeoPlatform ArcGIS Online as an additional resource.

The GeoPlatform uses Login.gov as an identity provider and uses the Keycloak platform for identity management and user federation services. Keycloak's user federation services allow GeoPlatform to provide one sign-in option for users signing in with a Login.gov account using one of the following authentication methods: Personal Identity Verification (PIV) card, Common Access Card (CAC) or two-factor authentication. Keycloak manages the federation behind the scenes and is accessible to authorized administrators only. Keycloak maintains a reference to the user's unique identifier, email, first name, and last name and requires the user to verify their email before access is granted. GeoPlatform ArcGIS Online https://geoplatform.maps.arcgis.com uses Login.gov to support users signing in with a PIV card, CAC, or email and password plus a chosen two-factor authentication method. Login.gov is a General Services Administration (GSA) system that was assessed in a separate privacy impact assessment (PIA) and is not included in this PIA. The Login.gov PIA may be viewed on the GSA PIA website at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

C. What is the legal authority?

Geospatial Data Act of 2018 (GDA); Cloud First Policy; Data Center Optimization Initiative (DCOI); E-Government Act of 2002; Executive Order 12906, *Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure*, amended by Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*; Executive Order 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*; OMB Circular A-16, *Coordination of Geographic Information and Related Spatial Data Activities*; OMB Circular A-130, *Managing Information as a Strategic Resource*; and OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*; OMB M-19-19, *Update to Data Center Optimization Initiative,* June 25, 2019; NIST SP 500-292*, NIST Cloud Computing Reference Architecture,* September 08, 2011; and NIST 800-53 Rev 5*, Security and Privacy Controls for Information Systems and Organizations*

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*

010-999993100; GeoPlatform System Security and Privacy Plan

☐ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	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)*
☒ No

GeoPlatform does not create records about individuals within the system, however, user accounts are created and managed through Login.gov, a secure authentication service managed by GSA, which is covered by the GSA system of records notice (SORN), GSA/TTS-1, Login.gov. DOI does not receive or manage user accounts from login.gov. See the GSA/TTS-1 SORN and Login.gov PIA on how GSA manages user data.

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
☒ Personal Email Address
☒ Other: *Specify the PII collected.*

GeoPlatform supports Login.gov as an identity provider. Upon initial log in to GeoPlatform ArcGIS Online with a Login.gov account (also referred to by some users as a USA Jobs account), Keycloak captures the individual's Login.gov account first name, last name, and email address to include personal email addresses.

GeoPlatform CHS through its contracted cloud broker provides authorized GeoPlatform cloud customers with access to the AWS Management Console using AWS Identity and Access Management (IAM) policies. AWS IAM is the automated mechanism for managing AWS (infrastructure) user accounts and access policies. A baseline set of AWS IAM groups and roles with associated access policies support the alignment of an authorized user's account to personnel functions related to the management of the infrastructure such as billing for Federal agency customers and organizations within DOI, Elastic Compute Cloud (EC2), Virtual Private Cloud (VPC), Relational Database Service (RDS), Information Technology (IT) auditing, etc. Access to billing information in the AWS Management Console provides the GeoPlatform cloud customer with an at-a-glance view of their AWS infrastructure to understand AWS spending / utilization and view and pay invoices. GeoPlatform uses IAM to control access to AWS services and adds specific conditions such as originating IP address, user permissions and multifactor authentication. AWS built-in features employ transport layer security (TLS) for console access. Console access is for privileged users and for performing administrative tasks, TLS is enforced for all connections accessing GeoPlatform. GeoPlatform uses a Least-Privilege Policy for granting access. GeoPlatform retains the user's first name, last name, and email address and in special conditions, the user's originating IP address.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency – Login.gov is managed by GSA
☒ 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*

GeoPlatform utilizes Keycloak to manage authentication and user account management for approved applications and GeoPlatform ArcGIS Online when logging in with Active Directory Federation Services (ADFS) or Login.gov accounts (providing access to CAC and PIV cards). User account information collected by the federated identity services is sent directly to Keycloak in a user-initiated, machine-to-machine transaction. Users may also contact the GeoPlatform Service Desk by email when needing assistance with their existing account or to request how to get a new user account.

To learn more about how GeoPlatform ArcGIS Online uses the PII collected as it pertains to each of the remaining questions in this PIA, please see https://www.doi.gov/sites/doi.gov/files/uploads/arcgis-online-pia-final-04072020.pdf.

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

GeoPlatform uses the PII to establish the user's identity and to provide user credentials for access to the AWS console to access billing and AWS utilization information for managing the cloud customer's AWS infrastructure.

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 will be shared with the DOI Office of the Chief Information Officer (OCIO) who is the managing partner of GeoPlatform on behalf of the FGDC and its member agencies.

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

The GeoPlatform is available to DOI Bureaus and FGDC member agencies to host geospatial projects in GeoPlatform's CHS. GeoPlatform.gov is available to the public and any bureau or agency to search, discover, and use published geospatial data and services. GeoPlatform only shares the information the user provides with another government agency if the user's question relates to that agency, or as required by laws. GeoPlatform never collects information, creates or shares individual profiles for commercial marketing.

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

The GeoPlatform is available to DOI Bureaus and FGDC member agencies to host geospatial projects in GeoPlatform's CHS. GeoPlatform.gov is available to the public and any bureau or agency to search, discover, and use published geospatial data and services. GeoPlatform only shares the information the user provides with another government agency if the user's question relates to that agency, or as required by laws. GeoPlatform does not collect information, create or share individual profiles for commercial marketing.

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

The business model for the GeoPlatform emphasizes a partner network of providers including Federal agencies and their partners in state local, regional, and tribal governments, non-profit organizations, academic institutions, industry, and citizens. GeoPlatform may share the information the user provides with other government entities if the user's question relates to that government entity, or as required by law. GeoPlatform does not collect information, create or share individual profiles for commercial marketing.

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

User account profile information may be shared with DOI contractors to communicate with users and support the GeoPlatform program.

☐ 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.*

The website, GeoPlatform.gov is a public website where users can browse the website data anonymously. There is a privacy policy pertaining to the collection of information from the users posted at https://kb.geoplatform.gov/gc-dataandprivacypolicies.html#privacy-policy that the users can review.

☐ 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.*

There is a privacy policy pertaining to the collection of information from the users posted at https://kb.geoplatform.gov/gc-dataandprivacypolicies.html#privacy-policy that the users can review. Users creating an account are referred to Login.gov. Privacy Notice for Login.gov is provided by GSA through the GSA Login.gov PIA and GSA/TTS-1 SORN, and privacy policy. Government users of the cloud service can view AWS's Privacy Policy located at https://aws.amazon.com/privacy/.

☒ Other: *Describe each applicable format.*

Individuals are also provided notice through the publication of this PIA.

☐ None

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

GeoPlatform may retrieve the user's name and username through the AWS console to review and manage privileged user access. As an option, a tag with the user's email may be added.

I. Will reports be produced on individuals?

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

AWS Console IAM Privileged Users – Data is retrieved manually by an administrator and submitted monthly to the GeoPlatform Executive Management Team. Role-based account strategy has been established for access to GeoPlatform and access to enhanced security functions and is monitored in accordance with DOI Access Management guidelines and DOI Security Standard requirements. GeoPlatform generates monthly reports of privileged accounts for the purpose of monitoring privileged access and any unauthorized changes to privileged users and authorized access. GeoPlatform Management and Support Teams review and reconcile monthly reports and any unauthorized privileged account changes, or modifications are investigated accordingly. Account modifications are logged in accordance with GeoPlatform audit filtering strategy and changes to privileged accounts or access to security functions are logged and reviewed to ensure proper authorization.

☐ No

Section 3. Attributes of System Data

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

Geospatial data is collected from geospatial metadata records reported to Data.gov by the member agencies of the FGDC. Data.gov's open-source Comprehensive knowledge Archive Network (CKAN) catalog replaces two separate catalogs for Data.gov and GeoPlatform.gov and becomes a single-entry point for the users to search all the available open government data. The CKAN Catalog User Interface enables the discovery of data based on "search facets" which are fields that may be selected by a user to rapidly focus on topics, sources, and locations, and the Rich Application Programming Interface (API) allows the developers to further refine the search and presentation. GeoPlatform data is pulled from Data.gov using Data.gov's open and published API. GeoPlatform's data quality attributes along with use constraints are described in the metadata record associated with the data via Data.gov. The data owners are responsible for their metadata records as well as the accuracy of the datasets they publish.

B. How will data be checked for completeness?

GeoPlatform has an application process for data validation. The data validation standards conform with the Geospatial metadata requirements set by FGDC in accordance with the standard prescribed by the International Organization for Standardization (ISO).

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

In accordance with the Open Data policy, Federal agencies may publish metadata records to an internet-accessible open data site on the agency's website. The Data.gov catalog "harvests" these records from the agencies once a week from the agencies' web-accessible folders, and the data sources of GeoPlatform are collected on a weekly basis. The data owners are responsible for their metadata records as well as the currency and quality of the datasets they publish.

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

Original geospatial data is unscheduled and regarded as permanent records.

Backup data are maintained under Departmental Records Schedule (DRS) 1.4A, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-00013), which has been approved by the National Archives and Records Administration (NARA). The disposition of these records is temporary, and the records are cut off when the backups are superseded by a full backup, and when no longer needed for system restoration. The data will be destroyed no later than 3 years after cutoff. The same retention schedule applies to the user identification, profiles, authorizations, and password files. The disposition is temporary, and records are cut off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

Records maintained in GeoPlatform that belong to member agencies are retained in accordance with applicable agency records retention schedules or General Records Schedules approved by NARA, and members are responsible for managing and disposing of their own records.

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

Each member agency storing data in the system maintains those records under NARA approved records schedules for the retention of reports and data. DOI records are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental Policy.

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

There is a limited privacy risk to users who are granted access to GeoPlatform ArcGIS Online and are authenticated through Login.gov. There is an increased privacy risk for users who use their personal email for Login.gov due to the PII collected by system administrators which include departmental and DOI contractor staff to manage user accounts and authenticate users for access to GeoPlatform ArcGIS Online. This risk is mitigated by a combination of technical, physical, and administrative controls. The system administrators that create and manage user accounts are DOI employees and contractors who have signed the DOI Rules of Behavior and are subject to monitoring. DOI employees must complete Information and Management Technology (IMT) awareness training which includes privacy, cybersecurity, records management, Controlled Unclassified Information (CUI), Section 508, and the Paperwork Reduction Act (PRA) and the DOI Rules of Behavior prior to 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. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties. Users are also advised not to share sensitive information and the system administrators periodically review user content to ensure compliance with DOI security and privacy policies.

There is a risk that individuals may provide PII or geographical information deemed to be sensitive in nature. These risks are mitigated by using the least privilege principle when assigning a role to a user's account. System administrators also conduct a review user content periodically and when a user requests to share content publicly. Users with privileged accounts are required to read and sign the GeoPlatform Rules of Behavior and Access Policy for Privileged Accounts.

There is a risk that the individual may not know or consent to the uses of their information once it is collected. Individuals can review the GeoPlatform data and privacy policies which may be viewed at https://kb.geoplatform.gov/gc-dataandprivacypolicies.html on how their information will be used. Individuals can also refer to this GeoPlatform PIA. Users referred to Login.gov are provided with a Privacy Notice by GSA and may also view the GSA Login.gov PIA and GSA/TTS-1 SORN for how their information is used.

GeoPlatform's CHS provider is FedRAMP certified and uses NIST SP 800-53 security controls and follows NIST guidelines in implementing and managing its security policies and privacy controls. The transmission of the data is protected using secure-based protocols, and the data stored is protected through locally encrypted device management. GeoPlatform is rated as FISMA Moderate based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. In addition, all DOI employees and contractors must complete privacy, security and records management awareness training, as well as role-based training where applicable on an annual basis and sign the DOI Rules of Behavior prior to accessing the system.

There is a risk that the PII system data may be maintained longer than necessary. This risk is mitigated by DOI's enforcement of records management processes. Records are maintained and disposed of in accordance with records retention schedules that were approved by NARA and personnel are reminded through policy and annual training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

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 system aggregates geospatial data and makes it available to the public which helps agencies meet their mission needs, including communicating with and sharing data with the public. The information collected about the users would only be used to facilitate the users' active interaction on GeoPlatform.gov.

☐ 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. GeoPlatform 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*

System administrator accounts can manage user privileges and restrictions. Remote access to the GeoPlatform infrastructure is based on the least privilege principle. Access is provided through a whitelist and requires two-factor authentication. Database servers and clusters are not accessible via remote terminal. Remote terminal access is provided to those system administrators that perform regular maintenance, operating system updates, patches, and software deployments.

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

GeoPlatform.gov is a public-facing website that harvests geospatial records from Data.gov and allows users to search all records without the need for a user account.

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?*

The following privacy clauses are included in the contract. The contract will be updated to include the appropriate privacy clauses.

- FAR 52.224-2 Privacy Act (APR 1984)
- FAR 52.224-1 Privacy Act Notification (APR 1984)
- FAR 52.239-1 Privacy or Security Safeguards (AUG 1996)
- FAR 52.224-3 Privacy Training (JAN 2017) and Alternate I (JAN 2017) of 52.224-3

☐ 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*

AWS CloudTrail is the automated mechanism for logging and monitoring activity of all users in the environment. CloudTrail will produce logs containing the type of event that occurred, where the event occurred, when the event occurred, the source of the event, the outcome of the event and the identity of any individuals or subjects associated with the event.

☐ No

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

To manage and monitor the website, the web server logs record and track the users' access to the website, including the information about the page the user is entering the site from and the page the user is landing on. The web statistics also monitor how long a user stays on the site.

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

Internal access to the system is restricted to authorized personnel. In addition, all DOI employees and contractors must complete privacy and security awareness and role-based training, and records management training prior to being granted access to any DOI information technology resource annually, and sign 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*

The GeoPlatform is a cloud-based system that is maintained by AWS East/West as part of the requirements reviewed and determined by FedRAMP. AWS is FedRAMP certified and implements the NIST SP 800-53 security controls.

(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*

AWS is FedRAMP certified and is required to implement the NIST SP 800-53 security controls.

(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*

AWS is FedRAMP certified and is required to implement the NIST SP 800-53 security controls.

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 Geospatial Information Officer, Information & Technology Management Division, Office of the Chief Information Officer serves as the GeoPlatform Information System Owner and the official responsible for oversight and management of security controls and the protection of information processed and stored in the GeoPlatform system. The Information System Owner and the 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 in GeoPlatform, in consultation with the Departmental Privacy Officer.

The System Owner, on behalf of DOI as the managing partner of FGDC, and FGDC, is responsible for protecting the privacy rights of the public for the information collected, maintained, and used in the GeoPlatform system, and for meeting privacy requirements and addressing complaints.

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 GeoPlatform Information System Owner is responsible for daily operational oversight and management of the GeoPlatform’s security and privacy controls and 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 GeoPlatform Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI’s incident reporting portal, and appropriate DOI officials in accordance with Federal policy and established procedures, including the DOI Privacy Breach Response Plan.