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 Secretary
Date: October 2, 2017
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 an online portal used to share geographic data, maps, and online services. It is a strategic national resource that supports the Federal Administration's Open Government, Open Data and Digital Government strategies to enhance transparency, collaboration and participation. GeoPlatform provides a suite of well-managed, highly available, and trusted geospatial data, services, and applications for use by Federal agencies and their State, local, tribal, and regional partners to meet their mission needs and the broader needs of the Nation. GeoPlatform was developed

by the member agencies of the Federal Geographic Data Committee (FGDC) through collaboration with partners and stakeholders and is implemented to help agencies meet their mission needs, including communicating with and publishing data and maps to the public. GeoPlatform focuses on web applications that facilitate participatory information sharing, interoperability, user□centered design, and collaboration on the World Wide Web. GeoPlatform is a key component connecting many goals of the National Spatial Data Infrastructure (NSDI) Strategic Plan in advancing the NSDI. The portfolio of data, applications, and services provided on the GeoPlatform is stewarded through the use of open licenses and careful review. It is hosted on a cloud infrastructure, an Infrastructure as a Service provided by the Amazon Web Services (AWS) that maximizes geospatial interoperability. GeoPlatform provides streamlined access to National Geospatial Data Assets and reduces data duplication. The collaborative GeoPlatform Marketplace which provides a listing of datasets that are planned for acquisition by one or more of the FGDC member agencies helps reduce data acquisition costs. GeoPlatform's tools and dashboards support the Office of Management and Budget (OMB) Circular A-16, *Coordination of Geographic Information and Related Spatial Data Activities*, portfolio management process.

GeoPlatform is managed by the Department of the Interior (DOI), a partner of FDGC that is composed of agency members responsible for the National Geospatial Data Asset (NGDA) Themes as designated in OMB Circular A-16, Appendix E. The GeoPlatform system has continuously provided greater reliability and availability to the Geographic Information System (GIS) data and enables both DOI and the FGDC members that produce, maintain or use spatial data either directly or indirectly to successfully fulfill their mission with a coordinated and effective Federal geospatial asset management capability.

C. What is the legal authority?

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*.

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 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

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.gov collects the email addresses (personal or work), username, and the full names of the users and the names of the organizations the users work for when the users create an account with GeoPlatform. Users have the option of not providing the information of their organizations when registering for an account. The users can also view the GeoPlatform.gov website anonymously without creating an account. In addition, GeoPlatform.gov collects the date and time of access, the Internet address of the website from which the user was directed to GeoPlatform.gov, the name of the file or words the users searched, the items the users clicked on a page, and the browser and operating system the users used.

The information that the users compile can be tagged with the names or email addresses of the users. The system also maintains credentials of the system administrators for them to access and manage the system through multi-factor authentication process.

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*

GeoPlatform might collect information from stakeholders who are:

- Partners: 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. Partners provide geospatial assets including data, services, applications, and infrastructure to the GeoPlatform. In return, partners receive hosting capacity, technical support, and exposure of services to the broader community.

  The partners are governed by "rules of engagement" included in negotiated contractual, license, or service-level agreements.

- Users and communities: GeoPlatform users include geographic information systems professionals as well as a broad range of consumers of geo-data. The user community may include government decision makers and geospatial experts, emergency response planners, environmental advocates, special interest groups, scientists and enthusiasts, entrepreneurs and innovators, transit authorities, meteorologists, endangered species advocates, and more. The GeoPlatform is also a resource for members of the general public, who may access geospatial data and maps that are relevant or of interest to them.

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*

Users may register for an account through https://www.geoplatform.gov/about or https://idp.geoplatform.gov/registeruser.html.

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

GeoPlatform uses the user's information to establish the user's identity and to provide user credentials for access to the GeoPlatform. User credentials are also used to assign these individuals to specific data communities within the GeoPlatform. Once the user logs into GeoPlatform, the user may use their identity to gain access to certain data communities with authorized access right to compile data from different data sources or data communities, and to manage or share the geospatial products that the user creates by utilizing and interacting with the GeoPlatform domain.

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.

GeoPlatform uses the user's information to establish user identity and user credentials to access GeoPlatform. User's credentials are also used to assign users to specific communities within GeoPlatform. Users only have access to authorized communities. The user account information allows GeoPlatform and the users to interactively manage the products the users create and to satisfy the specific needs of the users through a tailored approach.

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

GeoPlatform is available to the public and any bureau or agency to search, discover and use published geospatial data and services. As an option, the user can provide an email address and username to create an account in GeoPlatform.gov. GeoPlatform only share the information the user provides with another government agency if the user's question relates to that agency, or as required by law. GeoPlatform.gov 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.*

GeoPlatform is available to the public and any bureau and agencies to search, discover, and use published geospatial data and services. The user can provide an email address and username for the optional uses of GeoPlatform.gov. GeoPlatform only shares the information the user give with another government agency if the user's question relates to that agency, or as required by law. GeoPlatform.gov does not collect, create or share an individual's information 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.

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

Limited numbers of staff that manage the Image Matters of GeoPlatform under the FGDC contract have access to the user ID of the website users for the purpose of maintaining the site function. These individuals do not have access to or manage the user account. The system administrators may access user account information in order to assist and resolve user requests.

☐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 users have the option of either registering for an account or browsing the website data anonymously. There is a privacy policy pertaining to the collection of information from the users posted at https://www.geoplatform.gov/privacy that the users can review then choose to either decline or consent to the collection of user information by GeoPlatform.gov.

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

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

☐Privacy Act Statement: *Describe each applicable format.*

☒Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the GeoPlatform Privacy Policy at https://www.geoplatform.gov/privacy when registering for an account.

☒Other: *Describe each applicable format.*

Individuals are also provided notice through the publication of this privacy impact assessment.

☐None

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

The system administrators and the community managers have access to the user's names and email addresses through an administrative dashboard to review and manage user access to specific communities.

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?

Geospatial data is collected from geospatial metadata records reported to Data.gov by the Federal agencies which are the members 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 become 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 data's 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.

The GeoPlatform is a public access site. The user's information will be updated upon request when there are changes to the user's account information. Based on the trackable membership records, FGDC will review the information of the community owners on a quarterly basis to ensure the record is up-to-date and the Federal employee status of the community owners remain unchanged.

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

The data in GeoPlatform include the original data and the backup data. The 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 cut-off. 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 384 Departmental Manual 1.

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

There is moderate risk to the privacy of individuals due to the PII collected, used and maintained in GeoPlatform. GeoPlatform collects username, personal or work email address and the organization name from all the users, including members of the public and the Federal employees working on behalf of the Federal agency that are members of the FGDC for the purpose of facilitating users' access to the open geo-data. GeoPlatform has implemented privacy and security controls to ensure that individual privacy is protected and privacy risks are minimized. GeoPlatform implemented a PII collection and consent process by providing a privacy policy that provides notice to users when registering for an account. The GeoPlatform privacy policy is posted on the website to provide transparency and accountability on GeoPlatform's collection, use, maintenance, and disposition of the related information.

GeoPlatform also ensures that the user accounts are properly managed, user access are properly authenticated and authorized, and user information collected will only be used for the defined purposes and may only be accessed by the authorized personnel. GeoPlatform has a process to deactivate a member's user account due to user account inactivity after 90 consecutive days, and deactivate an administrator's access after 30 consecutive days of inactivity. The customer agency's representative users' access roles on the account will be removed based on customer agency notifications, and the account remains deactivated for audit and historical purposes unless the customer agency terminates the account after the expiration of the records retention period specified by the customer agency's record retention schedule.

The host service provider of GeoPlatform is FedRAMP certified, who uses the 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 through the use of secure based protocols, and the data stored is protected though 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.

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 publishing data and maps to the public. The information collected about the users would only be used to facilitate the users' active interaction through this online geospatial data services.

☐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.

☐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*

Users who register an account with GeoPlatform will have access to publicly available geospatial data to create geospatial data and modify only their authored geospatial data assets. Users may update their profile information but may not remove or delete their accounts without contacting the GeoPlatform helpdesk.

Contractors with a registered account have the same privileges as a user account. Contractor accounts with least privilege are added to the management group of communities in GeoPlatform. These rights entitle the contractor to add, edit, and delete content in a community content management system (CMS) page. System access via remote terminal is not determined by a contractor account.

Developers with a registered account have the same privileges as a user account. System access via remote terminal and administrative accounts are not determined by the developer.

System administrator accounts can manage user rights and restrictions for community CMS pages. 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 administers 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 is a public-facing website that allows users access to the data posted on the website by logging in to the data communities to compile geospatial data of interest. The data community manager has access only to the user account information of the users who are interested in joining that community for the purpose of granting and revoking user access. The system administrators are granted access to the user account information based on the least-privilege and need-to-know principle.

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?*

☐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*

Amazon cloudtrail provides capabilities to identify, locate, and monitor administrators providing support to the Amazon Web Services (AWS) console. All user access is logged and managed as part of that system process, and via the web server.

☐No

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

For the purpose of managing and monitoring 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?

Various security controls are in place that prevent automated crawling and entry on user forms, discourage aggressive web crawlers from heavily indexing the system, divert high load traffic, and obfuscate the actual information system service endpoints from external monitors, traffic, and malicious users. The user data is encrypted both at rest and in transit.

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 cloud based system is maintained by the AWS services 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. FedRAMP use 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. FedRAMP use 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.