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: DOI Cloud Website
Date: February 22, 2018
Bureau/Office: Office of the Chief Information Officer
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 Department of the Interior (DOI) Cloud Website is a collection of pages providing information and other resources related to cloud services provided by DOI. This is primarily focused on the Foundation Cloud Hosting Services (FCHS) contract and the DOI assisted acquisition services, but also includes general information about the DOI Geospatial Platform.

The DOI FCHS contract and assisted acquisition services are provided by the DOI Office of the Chief Information Officer (OCIO) and the Interior Business Center, Acquisitions Directorate (AQD). The site is hosted and maintained as a part of www.doi.gov and includes only non-restricted publicly available data. The DOI Cloud Website is at www.doi.gov/cloud.

Personally identifiable information (PII) is not collected directly from the public. Only Federal agency customer data is collected, stored or processed on the DOI cloud website. Federal customers requesting cloud hosting services may download the FCHS Contract form and submit via email to DOI to initiate the process. The only information collected in the forms that is specific to an individual is first and last name, organization, business email and business phone number. The remaining information collected in the form is specific to project requirements for customer intake.

The DOI Cloud Website is meant to help provide general information and guidance for Federal government agencies that are looking to procure cloud based services. The website is organized into multiple page collections in order to help guide visitors through the process visually. There is a collection of pages specific to the Federal "Cloud First" policy and other government specific information. There are also page collections providing information on DOI provided cloud services available to the Federal government.

The remaining page collections are for Frequently Asked Questions (FAQs) and templates pages. FAQs and templates are again primarily focused on the FCHS contract and instructions for use. All information published is unrestricted and available to the public. However, the services referenced on the DOI Cloud Website are only available to Federal government customers. There is an email provided (fchs-inquire@doi.gov) to contact the OCIO/AQD cloud team with questions or to submit a project request.

All sub-pages on the DOI.gov website include the link to the contact page which has a form to allow customers to submit feedback to the website administrator. The information collected is the name and email address along with any feedback provided. This information is used to respond back to customer feedback requests and is not shared outside of DOI.

C. What is the legal authority?

- OMB Circular A-130, *Managing Information as a Strategic Resource*
- Management of Federal Information Resources; Executive Order 13571
- “Streamlining Service Delivery and Improving Customer Service,” April 11, 2011
- Federal Cloud Computing Strategy, February 8th, 2011

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?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

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

UII Code: 010-000002181; No SSP

☐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
☒Other: *Specify the PII collected.*

The only PII collected on the contact us page is name, and email address of Federal employees contacting DOI through DOI.gov. PII may be included within the contents of the email message. The FCHS intake form that is downloaded and submitted to DOI collects name, Federal agency, office, title, official email address, official phone number, and details about the project.

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*

Information submitted in the feedback and customer intake forms on DOI.gov are submitted to DOI via e-mail in the DOI BisonConnect system.

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?

The name, official e-mail address and phone number of Federal agency employees are used to process customer intake forms, communicate and provide services. The provision of name and contact information is voluntary by the Federal agency customer to facilitate requested cloud hosting services and provide feedback.

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.*

Information from cloud intake forms, such as official name, email address and phone number, may be shared with other personnel and organization within a DOI bureau or office on a need-to-know basis to respond to customer requests. The data is not shared with anyone outside DOI.

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

The customer intake forms are received by the DOI Interior Business Center (IBC) Acquisitions Directorate (AQD). The information in the form is collected into the contract acquisition package used by AQD to manage the acquisitions process. All contract related information (digital and hard copy) is stored and managed securely in accordance with data protection standards for contract sensitive data.

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

Other Federal Agencies may submit intake forms related to a cloud project, which is received by the DOI IBC AQD. Communications related to requested cloud services may contain identifying information about the agency officials involved in the process such as name, title and official contact information.

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

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

Information may be shared with DOI credentialed contractors who perform administrative services or otherwise support DOI activities related to the system.

☐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 opportunity to request services or provide feedback is optional and is voluntarily made by Federal agency customers.

☐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.*

Privacy notice is provided through the publication of this privacy impact assessment. The DOI Cloud Website also contains a link to the DOI Privacy Policy, which provides information on DOI's privacy practices for visitors who visit DOI.gov (www.doi.gov/privacy).

☐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.).

All information used is related to official functions, personal information is not maintained or used to retrieve records. Federal agency customers may send emails to the OCIO/AQD cloud team at fchs-inquire@doi.gov with questions or to submit a project request. E-mails may also be received through the intake forms sent to the OCIO/AQD cloud team email address. Information from customer intake forms received by the IBC AQD is collected into the contract acquisition package used by AQD to manage the acquisitions process. All contract related information (digital and hard copy) is stored and managed securely in accordance with data protection standards for contract sensitive data.

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?

Federal agencies verify information on the intake form before submission. Also, the information collected from the agency employees will be verified and updated by acquisitions personnel during the procurement process. Data received from Federal agencies that complete the form is not verified or stored in the DOI Cloud website.

B. How will data be checked for completeness?

Federal agency customers are responsible for verifying completeness of intake forms or requests prior to submission.

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

Information collected will be updated each time a customer submits an intake form. Also, the information collected from these individuals will be verified and updated by acquisitions personnel during the procurement process. Timestamps are included in the emails for both the feedback and customer intake forms to help ensure timely responses to requests received.

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

The DOI Cloud Website System records are covered by DOI Departmental Records Schedule (DRS) 1.4. Short-term Information Technology Records, System Maintenance and Use, which is approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001-0013). The email records from BisonConnect have a temporary disposition and are determined obsolete when they are no longer needed for administrative, legal, audit, or other operational purposes, and destroyed no later than 3 years after cut-off. System administrator logs and other operational system records are covered by DRS 1.4.0013, System Maintenance and Use Records, which calls for retention for not more than 3 years after the close of the fiscal year in which the records were created.

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

Records are disposed of in accordance with the applicable records retention schedules for each type of record, Departmental policy and NARA guidelines. Paper records are shredded and records contained on electronic media are degaussed or erased in accordance with 384 Department 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.

Privacy risk is minimal as only Federal agency customer data is collected, stored or processed on the DOI Cloud Website. The only information collected in the intake forms that is specific to a Federal employee's name, agency or organization, business email, and business phone number. The remaining information collected in the form is specific to project requirements for customer intake.

Emails generated from the intake form and website are from Federal agency customers requesting DOI cloud hosting services. The DOI Cloud Website and sub-pages on the DOI.gov website include a link to the contact page which has a form to allow customers to submit feedback to the website administrator. The information collected include name and e-mail address along with any feedback provided. This information is used to respond back to customer feedback requests and is not shared outside of DOI.

There is a risk that a member of the public will visit the DOI Cloud website, submit an intake request form, or initiate contact with DOI. These visitors provide information to DOI during their visit to DOI.gov and any communications they initiate. The DOI Cloud Website provides information on the services offered and makes it clear that DOI supports delivery of cloud based and acquisition services to Federal agency customers government-wide in accordance with the Government Management and Reform Act (GMRA) of 1994. The DOI Cloud Website also contains a link to the DOI Privacy Policy, which provides information on DOI's privacy practices for visitors who visit DOI.gov (www.doi.gov/privacy). The DOI.gov website and all sub-pages also use session cookies for general session management, and to speed the browser experience and improve user experience. These cookies are temporary and are removed at the end of the web browser session or within a few days. Visitors may review the DOI Privacy Policy to learn what information is collected and how that information is handled.

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 purpose of the DOI Cloud Website is to provide information related to DOI cloud services and a process for Federal agency customers to request cloud hosting 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, new data is not collected.

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?

DOI bureau or office access to information from cloud intake forms, such as official name, email address and phone number, is limited to authorized personnel on a need-to-know basis to respond to customer requests and manage the acquisitions process.

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?*

Yes, the contracts used for website support include the required Privacy Act clauses.

☐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*

☒No

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

Not applicable. Monitoring of individuals is not performed.

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

The DOI FCHS team does not monitor individuals. Access to intake forms and other information submitted is limited to authorized personnel. Membership to the e-mail distribution groups used to collect feedback and intake forms is centrally controlled and managed, and is reviewed regularly to ensure information is not disseminated inappropriately.

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*

DOI Cloud Website is provided by and hosted by a FedRAMP certified service provider who has met all requirements for Physical Controls for information categorized as Moderate.

(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*

In addition to the DOI controls listed above, DOI Cloud Website is provided by and hosted by a FedRAMP certified service provider who has met all requirements for information categorized as Moderate.

(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 Information System Owner is responsible for oversight and management of security and privacy controls and ensuring the protection of data within the system. The System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies. The Information System Security Officer is responsible for continuous monitoring of security controls and ensuring the Information System Owner is informed of any issues or 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 Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.