U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior (DOI) 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 c onducting 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: Cloud Hosting Solutions Virtual Data Center (CHSVDC)
Bureau/Office: U.S. Geological Survey, Office of the Associate Chief Information Officer (ACIO)
Date: September 26, 2022
Point of Contact
Name: Cozenja M. Berry
Title: Associate Privacy Officer
Email: privacy@usgs.gov
Phone: 571-455-2415
Address: 12201 Sunrise Valley Drive, 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 U.S. Geological Survey (USGS) Cloud Hosting Solutions (CHS) provides virtual private cloud hosting services made available through a Virtual Data Center (VDC) that can be leveraged as needed by USGS application owners (users). Amazon Web Services (AWS) is the Cloud Service Provider (CSP) whose services are used to manage, and operate the VDC.

Different security requirements from the Federal Risk and Authorization Management Program (FedRAMP) apply to cloud services. The Cloud Hosting Solutions Virtual Data Center (CHSVDC) has been created as a system authorization boundary to manage USGS user access to AWS resources. Only Federal agency customer data is collected, stored or processed as part of the CHSVDC system boundary. Personally identifiable information (PII) is not collected directly from the public. USGS personnel requesting access to cloud services must complete an intake form that collects their 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 CHS provides information resources to support the USGS science mission and bureau internal operations. Each office/program utilizing CHS resources is responsible for ensuring proper use of CHS, and for implementation of privacy and security requirements through their authorized FISMA system boundary. Due to the nature of CHS, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, and briefing papers. CHS users are responsible for ensuring their application data is protected, and privacy impact assessments are conducted in coordination with the USGS Privacy Office as required by the E-Government Act of 2002.

CHS leverages AWS in the AWS East/West (US) regions. AWS East/West (US) Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) leverages the IaaS and PaaS cloud computing models as defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 (September 2011). The IaaS model enables convenient, on-demand Internet access to a shared pool of configurable AWS computing resources such as servers, storage, network infrastructure, applications, and various services. Customers can rapidly provision or release computing resources with minimal overhead or interaction with the cloud service provider. The PaaS model enables AWS to deliver hardware and software tools, needed for application development, to its customers as a service. A PaaS provider hosts the hardware on its own infrastructure. As a result, the PaaS frees the customer(s) from having to install in-house hardware and software to run a new application.

AWS East/West (US) is FedRAMP authorized and is currently used by several Federal agencies, including the Department of the Interior (DOI), Defense Information Systems Agency, Department of Defense, United States Department of Agriculture, National Aeronautics and Space Administration, Department of Justice, Department of Labor, General Services Administration and others for hosting and providing cost-effective, scalable, secure, and flexible infrastructure. Options are available to encrypt application data hosted within AWS East/West (US) both at rest and in transit as needed. Customers are responsible for ensuring their application data is protected through implementation of appropriate security and privacy controls.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 43 U.S.C. 1457: Duties of Secretary; 43 U.S.C. 31,

Director of United States Geological Survey; Public Law 116 – 207, Internet of Things Cybersecurity Improvement Act of 2020; Public Law 116-194, Information Technology Modernization Centers of Excellence Program Act; Federal Information Technology Acquisition Reform Act (FITARA) (2014); Federal Information Security Modernization Act (FISMA) (2014); Clinger Cohen Act (1996); Executive Order 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure; Executive Order 13571, Streamlining Service Delivery and Improving Customer Service; OMB Circular A-130, Managing Information as a Strategic Resource; Cloud First Strategy "Federal Cloud Computing Strategy", February 8, 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?

☒ Yes: 010-000002290; System Security and Privacy Plan (SSP) for Cloud Hosting Solutions Virtual Data Center

☐ 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

☒ No

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

☐ Yes

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: The following information is collected from users' enterprise active directory profile (Government employees and Contractors) when requesting CHSVDC services: Name, official email address, and work center. There is a potential that PII may exist in user data stored in CHS applications, which may include, but is not limited to, names, email addresses, telephone numbers, SSNs, 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. CHS users are responsible for ensuring that their application data is protected and PIAs are conducted for their systems in coordination with the Information System Security Officer for their FISMA system boundary and the USGS Privacy Office.

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*

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*

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

The name and official e-mail address 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: The information stored is only accessible by CHS team members.

☐ Other Bureaus/Offices.

☐ Other Federal Agencies.

☐ Tribal, State or Local Agencies.

☒ Contractor: AWS is a CSP that will manage the environment. Per contractual obligations, they have no authorization to review, audit, transmit, or store DOI data. DOI may have contractor support within program areas, and these contractors will have limited access to contents of the services in the system.

☐ Other Third-Party Sources.

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

☒ Yes: The opportunity to request services or provide feedback is optional and is voluntarily made by Federal agency customers.

☐ No

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

☐ Privacy Act Statement:

☒ Privacy Notice: Privacy notice is provided through the publication of this privacy impact assessment. The USGS Cloud Website also contains a link to the USGS Privacy Policies, which provides information on USGS' privacy practices for visitors who visit USGS.gov (Privacy Policies | U.S. Geological Survey (usgs.gov)).

☐ Other:

☐ 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 only key is the service request ticket number. PII information is not used to retrieve records.

I. **Will reports be produced on individuals?**

☐ Yes

☒ No

Section 3. Attributes of System Data

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

No data is accepted from sources other than USGS employees or USGS contractors. Information submitted by USGS employees or contractors on the intake forms for a CHSVDC service is verified for accuracy by the CHSVDC service management and/or operations team personnel before approving the service.

B. **How will data be checked for completeness?**

CHSVDC service management and/or operations team personnel review the intake forms for completeness before approving the service. If the information is incomplete, the USGS employees or contractors are informed via email and requested that they provide properly completed forms.

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

The service management team receives notification that is time-stamped when a CHSVDC form is submitted by USGS employees or USGS contractors for CHSVDC service. The service management team does have an SOP to process the request for CHSVDC services in an organized and efficient manner.

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 for managing the system is under the System Maintenance and Use Files under disposition authority number DAA-0048-203-0001-0013, item 4.1.1. The disposition for the data housed in the virtual data centers would be related to the content and will vary based on the Federal agency and other factors in accordance with approved records schedules.

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

Procedures for disposition of the data stored in individual applications will vary by office/program and needs of the agency. Due to the nature of CHS, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each office/program and user that creates or maintains federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area. Approved disposition methods include 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 minimal risk to the privacy of individuals for the use of CHSVDC due to the nature of the services. CHSVDC is constructed in AWS, which is a subscription service offering a shared pool of computing resources that includes a very limited amount of PII. The level of risk associated with the type and sensitivity of PII is dependent on the office or program use and the safeguards implemented to mitigate the risk. Information stored within CHSVDC system boundary may include name and email address of USGS employees and contractors.

The CHS provides information resources to support the USGS science mission and bureau internal operations. Each office/program utilizing CHS resources is responsible for ensuring proper use of CHS, and for implementation of privacy and security requirements through their authorized FISMA system boundary. CHSVDC provides services where users may store all types of electronic files including text, graphical, audio, or video 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 within their applications. There is a potential that large amounts of PII may be included in the records stored by users within their applications. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, SSNs, 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. Users are responsible for protecting privacy data that is stored within their application, and privacy impact assessments are conducted in coordination with the USGS Privacy Office.

To mitigate privacy risks related to unauthorized access, unauthorized disclosure or information used for unauthorized purposes, CHSVDC has implemented a series of administrative and technical controls. AWS is a FedRAMP-approved CSP and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. AWS 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. Prior to granting users access to the DOI network, all users must agree to the USGS Rules of Behavior, as well as the DOI Warning Banner before accessing the system, which includes the consent to monitoring, and restrictions on data usage. CHSVDC's user identity management processes include authentication with Active Directory (AD) or AWS Identity and Access Management (IAM) to control and manage access restrictions to authorized personnel on an official need-to-know basis. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels. The contract between USGS and AWS does not allow the service provider to review, audit, transmit, or store USGS data, which minimizes privacy risks from the vendor source. All USGS 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 USGS Rules of Behavior prior to accessing the system. Users of the system must also sign a CHSVDC Rules of Behavior which prescribes additional practices and security controls specific to the cloud technologies in use.

CHSVDC utilizes a combination of technical and operational controls to reduce risk in the CHSVDC environment, such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies. All users of the CHSVDC minor applications must have a DOI account and government issued personal identity verification (PIV) card to access CHSVDC. Internal USGS customers utilizing the Microsoft Office 365 service are responsible for implementing adequate controls to safeguard PII used or maintained within their environment as appropriate. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the CHSVDC environment, which will help the agency effectively maintain a good privacy and security posture for the system. The system security and privacy plan is reviewed annually to ensure adequacy of controls implemented to protect data.

There is a risk that individuals may not receive adequate notice on the use of their PII. Privacy notice is provided through the publication of this privacy impact assessment. The USGS Cloud Website also contains a link to the USGS Privacy Policies, which provides information on USGS' privacy practices for visitors who visit USGS.gov.

There is a risk that data in CHSVDC will be maintained for longer than necessary. This risk is mitigated by managing records in accordance with a NARA-approved records schedule.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: The purpose of collecting PII is to process request for use of 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

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable, new data is not collected.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

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

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

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 DOI's AD System and AWS IAM. Only authorized DOI personnel will have access to the system, and that access is based on least privileges to perform job duties. Users and administrators can grant access to other information based on mission need. By default, all users only have access to information that they create or add. CHS performs regular audits of the system access and user interactions within the system

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. The contracts used for CHSVDC 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.

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes.

☒ 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 CHSVDC team does not monitor individuals. Access to forms and other information submitted is limited to authorized personnel.

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. CHSVDC is provided by USGS and is hosted by a FedRAMP certified service provider (AWS) 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 USGS controls listed above, CHSVDC is provided by USGS and is hosted by a FedRAMP certified service provider (AWS) 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 boundary. 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. CHS users and the associated FISMA System Owner are responsible for protecting Privacy Act information collected and maintained within their applications.

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, Information System Security Officer, and Chief of Cloud Hosting Solutions are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team (CSIRT), preferably by the assigned Security Point of Contact, in accordance with Federal policy and established procedures. Each program/office and user utilizing the CHSVDC platform is responsible for ensuring the security of data maintained in CHSVDC and for meeting privacy and security requirements within the USGS. They are also responsible for immediately reporting any potential compromise of data in accordance with Federal and DOI privacy breach response policy.