**U.S. Department of the Interior**
PRIVACY IMPACT ASSESSMENT

## Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

**Name of Project:** U.S. Geological Survey - Enterprise Common Security Control System
**Bureau/Office:** U.S. Geological Survey/Office of Enterprise Information
**Date:** May 24, 2018
**Point of Contact:**
Name: Miriam Benham
Title: IT Specialist
Email: mgbenham@usgs.gov
Phone: (916) 278-3314
Address: 2030 University Drive East, Suite 400, Modoc Hall, CSUS, Sacramento, CA 95819

## Section 1. General System Information

### A. Is a full PIA required?

☒Yes, information is collected from or maintained on
- ☐Members of the general public
- ☒Federal personnel and/or Federal contractors
- ☒Volunteers
- ☐All

☐No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

### B. What is the purpose of the system?

The purpose of the Enterprise Common Security Control System (ECSCS) is to implement enterprise infrastructure management for and secure use of U.S. Geological Survey (USGS) computer networks, resources and information. The ECSCS system is composed of the following components:

Enterprise Active Directory (eAD)
The eAD provides enterprise support for the Department of the Interior's (DOI) integrated Active Directory Service to USGS computer systems. The primary services include: Secure Authentication, Group Policy Management, Directory Services, Naming Services, and Continuous Security Monitoring. This component interfaces with the DOI Enterprise Hosted Infrastructure system, whose Privacy Impact Assessment is available at https://www.doi.gov/privacy/pia#DW.

Electronic Domain Name System (eDNS)
The eDNS provides external domain name services to USGS computer systems with consistent and uniform policy, administration and user interface(s). This component interfaces with the DOI Enterprise Hosted Infrastructure system, whose Privacy Impact Assessment is available at https://www.doi.gov/privacy/pia#DW.

Simple Mail Transfer Protocol (SMTP)
The USGS SMTP mail relay provides the following services for USGS servers and appliances (relay clients):

- Relaying SMTP mail from internal SMTP servers and appliances to the Internet through DOI BisonConnect
- Relaying SMTP mail from DOI BisonConnect with a destination for internal addresses that do not have a mailbox on DOI BisonConnect
- Relaying SMTP mail from the Internet directly to internal domains

Enterprise Vulnerability Management System (eVMS)
The eVMS provides vulnerability management for USGS computer systems by conducting monthly vulnerability assessments of the USGS internal network, responding to DOI external assessments of USGS systems available to the public, monthly assessment and verification of Internet-accessible USGS systems, and on-demand security scans for security points of contacts.

Enterprise Security Applications Service (eSAS)
The eSAS provides protection to USGS web servers from malicious internet traffic and intrusion. Redundant application-firewall appliances (Barracuda) located at the USGS regional centers are configured to filter and report attacks of public web servers, load-balance high-volume web traffic, and camouflage the identity of web server software.

Enterprise Device Endpoint Protection (eDEP)
The eDEP provides protection for USGS computer systems against malware and network threats using Symantec Endpoint Protection client (SEP) and Manager (SEPM) software.

Computer Security Incident Response Team (CSIRT)

The USGS Computer Security Incident Response Team (CSIRT) works with the DOI Computer Incident Response Center  to identify, analyze, report, contain, resolve, and recover from security incidents.  USGS CSIRT uses DOI's incident response tracking system, Remedy.

Data at Rest (DAR)
The DAR provides implementation of the DOI-wide DAR project for USGS computer systems to ensure encryption requirements for sensitive data are met. DAR uses the DOI McAfee solution.  This component interfaces with the DOI Enterprise Data-at Rest Encryption system, whose Privacy Impact Assessment is available at https://www.doi.gov/privacy/pia#DW.

Active Directory Federated Services (ADFS)
The ADFS identity access solution provides a federated identity management solution that extends distributed identification, authentication, and authorization services to Web-based applications across organizational boundaries.

## C. What is the legal authority?

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; E-Government Act of 2002, as amended; 110 Departmental Manual 18.

## 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)*

010-000001022; Enterprise Common Security Control System

☐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**<br>*(Yes/No)* | **Describe**<br>*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)*

DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, which is currently being revised.

☐No

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

☐Yes: *Describe*
☒No

## Section 2. Summary of System Data

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

☒Name
☐Citizenship
☐Gender
☐Birth Date
☐Group Affiliation
☐Marital Status
☐Biometrics
☐Other Names Used
☐Truncated SSN
☐Legal Status
☐Place of Birth
☐Religious Preference
☐Security Clearance

☐Spouse Information
☐Financial Information
☐Medical Information
☐Disability Information
☐Credit Card Number
☐Law Enforcement
☐Education Information
☐Emergency Contact
☐Driver’s License
☐Race/Ethnicity
☐Social Security Number (SSN)
☐Personal Cell Telephone Number
☐Tribal or Other ID Number

☐Personal Email Address
☐Mother's Maiden Name
☐Home Telephone Number
☐Child or Dependent Information
☒Employment Information
☐Military Status/Service
☐Mailing/Home Address
☒Other: *Specify the PII collected.* User full legal name, system login name, work e-mail address, web home page address, work address, work phone number, other contact information, user access and permission rights, password hash values, HSPD-12 authentication, digital signature, encryption, and/or other NIST specified certificates, along with the date and time of signature retained on the signed document, and supervisor's name.

**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
☒Other: *Describe* The eAD continuously updates data across the DOI active directory domains.

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

PII is used in the creation and administration of USGS user accounts. ECSCS provides access control and user authentication for services, applications, and other network resources across the USGS environment using the provided information.

**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.*

DOI.net eAD root replicates user account information to USGS domain controllers for the purpose of network access enforcement.

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

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

The HSPD-12 program is a government-wide requirement managed by the General Services Administration and is subject to Federal requirements for participating agencies that involve sharing of data - see government-wide system notice GSA/GOVT-7: Personal Identify Verification Identity Management System, for additional information sharing activities. Some information may be shared with other Federal Agencies as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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

Information may be shared with Tribal, state, or local agencies as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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

Information may be shared with contractors who perform services or otherwise support DOI activities related to the EHI, and as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

☐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.*

Information is voluntarily provided by employees in order to obtain access to the USGS network and information systems. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the USGS network. If users decline to provide the required information upon employment at USGS they will not be given access to the network and may be unable to perform their duties.

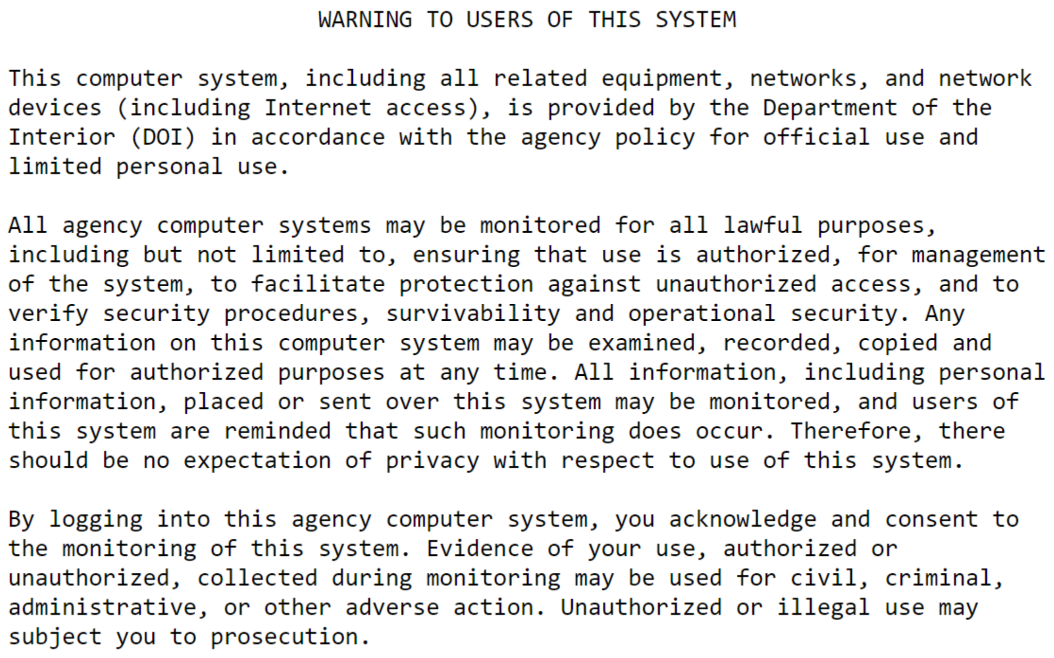
☐No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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



```
                        WARNING TO USERS OF THIS SYSTEM

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

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

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

☐Other: *Describe each applicable format.*

☐None

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

Data are retrieved by any defined field within the record. These fields include, but are not limited to: user name, full legal name, digital certificate, and Web home address or e-mail address.

**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?**

Not Applicable. PII is collected only from DOI records.

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

Specific account attributes within the eAD can be updated upon request of the user which would be primarily contact information.

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

Certain updates may take effect via the AD system updates, however; it is up to the individual to update their contact information and update data in any application and/or system that is hosted within ECSCS. USGS provides the eComputing Applications page where users can maintain and update their work related contact information. Users are notified that it is their responsibility to ensure their information is up to date. As a function of AD, all data related to user access is continuously synchronized across the entire system.

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

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

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

Once user accounts are terminated in the system, the records are removed in accordance with the GRDS and other applicable Bureau/office records retention schedules. Procedures for disposition of the data stored in individual applications will vary by application. When a user account is disabled or terminated in ECSCS, all access will be denied since the user will no longer have the ability to log onto or authenticate to the network. ECSCS user objects can be set to automatically expire at a given date to ensure that a user does not have access past the period of performance or contract. When the account is disabled, all access to the network and all ECSCS systems are explicitly denied, and all attempts to gain access are logged. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy, and National Archives and Records Administration guidelines.

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

There is a minimal privacy risk to individuals due to the limited information contained in the AD system and the mitigating controls implemented to protect data. Most of the PII includes employee name, username, work email address, work phone number, duty station address, and official title of USGS employees and contractors, and the work-related PII, such as contact information, duty station, and title, is not considered sensitive. System permissions and access controls are in place to limit system access to only those authorized individuals with a need to know the information to perform official functions.

ECSCS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. ECSCS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII contained in the system.

The ECSCS has developed a System Security Plan based on NIST guidance and is part of a Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on the ECSCS to identify and mitigate any found. Security and privacy awareness training is required for all USGS employees and information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter, and sign the DOI Rules of Behavior. Security role-based training is also required for security personnel and officials with special roles and privileges.

USGS complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Access to administrative functions is strictly controlled and can only be granted by USGS Domain Administrators. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource.

## Section 4. PIA Risk Review

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

☒Yes: *Explanation* PII is strictly used for identification and authentication access control purposes, and a subset of the information is used on a regular basis to conduct routine business within DOI.

☐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. No new data are being created.

**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.*

Data contained within AD are controlled by permissions and access is only granted to a few individuals with the correct level of permissions to view the data

☐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 and contractors will have access to their own information, and in some cases a limited subset of other users based on mission, system, and application management needs.

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

Access to data will be restricted through AD permissions and access controls. System administrators will have access based on a need to know and mission accomplishment.

**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 standard Privacy Act clauses are included in the contracts.

☐No

**J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?**

☐Yes. *Explanation*

☒No

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

☒Yes. *Explanation* Windows audit logs record this information for users by default and according to Security Technical Implementation Guide compliance.

☐No

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

As part of the security monitoring and management of the system user actions taken on ECSCS resources are audited and can be reviewed by Enterprise and Domain administrators. This information includes items such as: username, login date/time/location, failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

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

USGS complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any ECSCS equipment. The use of USGS IT systems is conducted in accordance with the appropriate use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Access to administrative functions is strictly controlled and can only be granted by domain administrators.  Additionally, users must be included in security groups assigned to a resource in order to access that particular resource. Also, all users must complete IT security and privacy awareness training, as well as role based training on an annual basis and before being granted access, and sign the DOI Rules of Behavior.

**N. How will the PII be secured?**

(1) Physical Controls. Indicate all that apply.

☒Security Guards
☒Key Guards
☒Locked File Cabinets
☒Secured Facility
☒Closed Circuit Television
☐Cipher Locks
☒Identification Badges
☐Safes
☐Combination Locks
☒Locked Offices
☐Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒Password
☒Firewall
☒Encryption
☒User Identification
☐Biometrics
☒Intrusion Detection System (IDS)
☒Virtual Private Network (VPN)
☒Public Key Infrastructure (PKI) Certificates
☒Personal Identity Verification (PIV) Card
☐Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒Periodic Security Audits
☒Backups Secured Off-site
☒Rules of Behavior
☒Role-Based Training
☒Regular Monitoring of Users' Security Practices
☒Methods to Ensure Only Authorized Personnel Have Access to PII
☒Encryption of Backups Containing Sensitive Data
☒Mandatory Security, Privacy and Records Management Training
☐Other. *Describe*

**O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.**

The ECSCS System Owner serves as the Information System Owner and the official responsible for oversight and management of ECSCS’s security and privacy controls, including the protection of information processed and stored by ECSCS. The Information System Owner and the ECSCS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by ECSCS. The System Manager is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the USGS Privacy Officer.

**P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?**

The ECSCS Information System Owner is responsible for oversight and management of the ECSCS security and privacy controls and for ensuring, to the greatest possible extent, that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team immediately upon discovery in accordance with Federal policy and established procedures.