U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior (DOI) requires Privacy Impact Assessments (PIAs) 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 - Earth Resources Observation and Science
Bureau/Office: U.S. Geological Survey/Earth Resources Observation and Science Center
Date: September 30, 2020
Point of Contact:
Name: Cozenja M. Berry
Title: Associate Privacy Officer
Email: cberry@usgs.gov
Phone: (703) 648-7062
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 purpose of the U.S. Geological Survey (USGS) Earth Resources Observation and Science (EROS) system is to provide administrative support and information technology (IT) to enable the EROS Center to accomplish its mission of using satellite images and other remotely sensed data to monitor, assess, and project how changes in land use, land cover, and land condition

affect people and nature. EROS is comprised of three subsystems: 1) EROS Science and Support Systems (CSAM ID 2264), 2) Land Satellites Data System Mission Operation Centers (CSAM ID 994), and 3) Landsat Data Systems Cloud (CSAM ID 244). The Land Satellites Data System Mission Operation Centers and the Landsat Data Systems Cloud do not collect personally identifiable information (PII) and a description of the services supported can be reviewed at https://lpdaac.usgs.gov/about/. Only one of these three subsystems, the EROS Science and Support Systems, contains PII.

The EROS Science and Support Systems is comprised of the following components:

1. Earth Explorer (EE): An online search, discovery, and ordering tool that contains millions of aerial and satellite images of the earth's surface; EE requires user registration on web server applications to order products.

2. Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER) Emergency Scheduling Interface and Control System (AESICS): ASTER is an instrument sensor onboard the Terra Earth Observing System satellite that captures data of the earth's surface. AESICS is a joint initiative between the USGS and the National Aeronautics and Space Administration (NASA) that enables users to order images taken from the ASTER instrument sensor in outer space. NASA Jet Propulsion Laboratory (JPL) is the managing partner for all user data in this system. AESICS requires user registration via EarthData Login, an application internal to the NASA controlled portal, http://eauth.mynasa.nasa.gov/(in the NASA Portal). User data is required to ensure that individuals have authenticated access to the website for delivery of data request and services. Public facing user profiles are administered by NASA, the managing partner, and complies with NASA's Web Privacy Policy. The PIA for the application http://eauth.mynasa.nasa.gov/ can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html (referred to as "application PIA" throughout this document).

C. What is the legal authority?

Executive Order 12906, Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure; Executive Order 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems; 33 USC 3404: Ocean exploration and undersea research technology and infrastructure task force; 51 USC 60101: Definitions; 51 USC 60142: Archiving of data; and OMB Circular No. A-16 Revised, Coordination of Geographic Information and Related Spatial Data 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.* This PIA realigns existing USGS subsystems under the EROS Assessment and Authorization boundary.

E. Is this information system registered in CSAM?

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

10-000001047 System Security and Privacy Plan for Earth Resources Observation and Science.

☐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.*
Unstructured Shared File Server	Data Storage-Record Retention	Yes	The shared file server may have information identified to an individual as well as financial data, however the data is owned, maintained, and administered by the program offices (file server users). Such data inherits the privacy controls for the program or application that it is associated with.
SQL Database Services	Data Storage	No	This application supports the distribution of data.
Web Server Applications	Data Distribution	No	Web server applications help projects share and distribute data.

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)*

EE: Records are covered by DOI under system of records notice, INTERIOR/USGS-18, Computer Registration System.

AESICS: NASA as the managing partner maintains their records under the NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User Information.

☐No

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

☒Yes: *Describe*

EE: Paperwork Reduction Act requirements are administered by USGS. The OMB Control number for this information collection is 1028-0119, Earth Explorer User Registration Service, Expiration Date: 8/31/2022.

AESICS: Paperwork Reduction Act requirements are determined and administered by NASA. Currently, there is no record of an OMB Control number for this information collection.

☐No

Section 2. Summary of System Data

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

☒Name
☒Home Telephone Number
☒Personal Email Address
☒Mailing/Home Address
☒Other: *Specify the PII collected.* Employee Email, Employee phone number, Company/Organization name, account credentials to access EROS and order products from EE.
Note: Home phone number, home address, and personal email may be provided by the user as their business contact in lieu of organization/employee information. PII is collected by NASA to access AESICS via EarthData Login - see the application PIA at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html.

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*

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

EE: In order for the USGS to distribute reproductions of remote sensing data from the archive, it is necessary to obtain the name, address, telephone number of customers in order to ship products and verify demographics for certain licensed product. EE was designed to capture and protect this information.

AESICS: PII is collected by the NASA JPL as the managing partner for the application. User data is required to ensure that individuals have authenticated access to the website for delivery of data request and services. NASA JPL manages AESICS order requests and makes data available to customers via EarthData Login, an application internal to the NASA controlled portal, http:// eauth.mynasa.nasa.gov/(in the NASA Portal).

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.*

EE and AESICS: The PII is shared with EROS personnel to process customer orders.

☐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.*

EE: Information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in the DOI system of records notice, INTERIOR/USGS-18, Computer Registration System.

AESICS: The data will be used by the NASA JPL to track order requests. Information may also be shared with other Federal agencies as authorized pursuant to the routine uses contained in

NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User 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.*

EE: Information may be shared with contractors who perform services or otherwise support USGS activities related to EE.

AESICS: Information may be shared with contractors who perform services or otherwise support USGS and NASA activities related to the AESICS.

☐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.*

EE and AESICS: Individuals can decline to provide their contact information but would be unable to receive their requested data without this information.

☐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 Act Statements are available to users during the account registration process for both EE and AESICS.

☒Privacy Notice: *Describe each applicable format.*

Privacy Notice is provided to individuals through the publication of the PIAs and the associated SORNs by USGS and NASA.

☐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.).

EE: Authorized individuals with specifically granted access to Privacy Act data retrieve the data by account number or order number.

AESICS: Name, email, and organization are retrieved automatically by the application when orders are placed.

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?

EE and AESICS: All fields will only be provided by the customer and is presumed to be accurate. For EE, an email is sent to new registered users to validate their email address.

B. How will data be checked for completeness?

EE: EE requires certain fields to be completed such as name, address, city, and zip code, before an account can be established and an order can be submitted.

AESICS: The data in the EarthData login is managed by NASA personnel. User profiles are administered by NASA and complies with NASA's privacy policy. The application PIA can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html.

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

EE: Updates are provided by the customer and are their responsibility to maintain. The customer is required to review submitted information annually.

AESICS: The data in the EarthData login is managed by NASA personnel. User profiles are administered by NASA and complies with NASA's privacy policy. The application PIA can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html.

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

EE: User registration records are maintained under the USGS General Records Disposition Schedule, Item 202-06b - User Identification, Profiles, Authorizations, and Password Files, Excluding Records Relating to Electronic Signatures. The disposition of these records is temporary, and the records are destroyed when the Bureau determines they are no longer needed for administrative, legal, audit, or other operational purposes.

AESICS: User registration required for EarthData login is managed by NASA. The records retention is addressed in the associated NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User Information and the application PIA which can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html. Guidance on NASA procedures for records management is addressed in the agency policy directive, NASA Records Management, NPD 1440.6I (https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1440_006I_&page_name=main&search_term=records%20dispostion).

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

EE: System administrators dispose of DOI records by shredding or pulping for paper records, and degaussing or erasing for electronic records in accordance with NARA Guidelines and 384 Departmental Manual 1. Procedures are documented in the Media Protection (MP) Standard Operating Procedures document.

AESICS: The data in the EarthData login is managed by NASA. The records disposition is addressed in the associated NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User Information and the application PIA which can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html. Guidance on NASA procedures for records disposition is addressed in the agency policy directive, NASA Records Management, NPD 1440.6I (https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1440_006I_&page_name=main&search_term=records%20dispostion).

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 privacy risk to users who are granted access to EE and AESICs due to PII collected to administer user accounts and authenticate access to the system. There may be risks related to the unstructured data containing PII that is maintained by USGS information owners who are responsible for ensuring appropriate controls are implemented to protect the data. During all phases of the information lifecycle, the principle of least privilege is observed. There is a risk that data may be inappropriately accessed or used for unauthorized purposes. In an effort to protect

the privacy of individuals, the minimal amount of PII is collected from users. These risks are mitigated by a combination of technical, physical and administrative controls. EROS has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. EROS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

Potential privacy risks include inadvertent disclosure, unauthorized surveillance, and theft. Such disclosure could reveal details of an individual's geolocation and contact information. PII is stored and maintained on internal systems only. It is protected from unauthorized access by firewalls, intrusion detection systems, antivirus programs, and the inherent security of the Active Directory domain environment. To mitigate the insider threat, collected data is protected by a combination of user ID, user password, and limited restricted access. USGS employees are required to complete the yearly Information Management and Technology Awareness Training, which includes affirming the USGS Rules of Behavior. Audit logs for the data are reviewed regularly for anomalies. USGS computers are secured and scanned in accordance with the USGS Continuous Monitoring Program Plan. The data is not shared outside the USGS/DOI, except as identified in the routine uses contained in DOI system of records notice, INTERIOR/USGS-18, Computer Registration System and NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User Information.

NASA implements security and privacy controls for AESICS ensuring compliance with Federal privacy laws and regulations throughout the information lifecycle. The privacy risks are addressed in the associated NASA system of records notice, GSFC 51EUID -Earth Observing System Data and Information System (EOSDIS) User Information and application PIA which can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html. NASA's policies for information security are addressed in the agency policy directive, NASA Information Security Policy, NPD 2810.1E (https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2810_001E_&page_name=main&search_term=information%20security).

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 data is relevant and necessary to ensure users have access to the EE and AESICS applications. The account registration allows users to save search criteria to be used for future reference. The account registration also provides the flexibility for managing licensed data received from another organization that requires specific licensing agreements for distribution.

Standing request services provide the capability for saving search criteria to a standing request. The standing request searches the inventory for new data that fulfills the first responder's area of interest and date/time requirements. Users are then automatically notified when the data is available for download. The standing request feature immediately provides disaster responders with data based on their area of interest to support the event.

☐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; EE and AESICS do not derive new data or create previously unavailable data about individuals through data aggregation.

F. Are the data or the processes being consolidated?

☐Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒No, data or processes are not being consolidated.

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

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

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

User access is restricted to their account registration information and their request for data and services. Users do not have access to the PII or other user data.

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?*

EE: USGS ensures Privacy Act contract clauses are included in contracts for EE.

AESICS: NASA administers its agency contracts related to AESICS and has oversight of the inclusion of Privacy Act clauses as required.

☐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*:

User monitoring is limited to information provided in system and web logs for system security administration purposes only.

☐No

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

IT audit logs include username, hostname, logon dates, times of failed logon attempts, IP addresses, webpages accessed, processes accessed and other system failures.

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

EE: The USGS complies with the National Institute of Standards and Technology and other Federal requirements for data security as part of a formal program of Assessment and Authorization, and continuous monitoring. Periodic 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 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. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource. USGS personnel with system administrator access must complete IT security and privacy awareness training as well as role-based training before being granted access to the system, when required by system changes, and at least annually thereafter.

AESICS: NASA implements security and privacy controls to prevent unauthorized monitoring for AESICS. Information security procedures are addressed in the associated NASA system of records notice, GSFC 51EUID - Earth Observing System Data and Information System (EOSDIS) User Information and application PIA which can be viewed at https://www.nasa.gov/privacy/PIA-eauth-mynasa-nasa-gov.html. NASA's policies for information security are addressed in the agency policy directive, NASA Information Security Policy, NPD 2810.1E (https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2810_001E_&page_name=main&search_term=information%20security).

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* SIEM for log collection and security monitoring.

(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.

EE: The Director, USGS EROS is the EROS System Owner and the official responsible for oversight and management of EROS's security and privacy controls, including the protection of information processed and stored by EROS. The Information System Owner and the EROS

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 EROS. 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 Associate Privacy Officer (APO). Specific guidance on how DOI implements the Privacy Act has been published to the Code of Federal Regulations at 43 CFR Part 2, Subpart K (https://www.ecfr.gov/cgi-bin/text-idx?SID=c42fde6e4d802ca59574c5ec3bcc5057&mc=true&node=pt43.1.2&rgn=div5#sp43.1.2.k).

AESICS: NASA, as the system administrator for AESICS, is responsible for the oversight and management of the system security and privacy controls including the protection of information processed and stored in the application. Specific guidance on how NASA implements the Privacy Act has been published to the Code of Federal Regulations at 14 CFR 1212 (https://www.govinfo.gov/content/pkg/CFR-1999-title14-vol5/xml/CFR-1999-title14-vol5-part1212-subpart1212-2.xml).

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?

EE: The EROS Information System Owner is responsible for oversight and management of the EROS 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. Incidents involving PII must be reported to the USGS APO and are managed in accordance with procedures outlined in the DOI Breach Response Plan. The APO oversees breach reporting and response activities to include incident investigation, mitigation efforts, and implementing corrective actions following a breach.

AESICS: NASA, as the managing partner for AESICS, is responsible for the oversight and management of the system 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. Guidance on NASA procedures for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information is addressed in the agency procedural requirements, NASA Privacy Procedural Requirements, NPR 1382.1A (https://nodis3.gsfc.nasa.gov/npg_img/N_PR_1382_001A_/N_PR_1382_001A__Chapter8.pdf).