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.

Name of Project: Reclamation Information Sharing Environment (RISE)
Bureau/Office: Bureau of Reclamation/Denver Office
Date: September 30, 2024
Point of Contact:
Name: Regina Magno
Title: Associate Privacy Officer
Email: privacy@usbr.gov
Phone: 303-445-3326
Address: PO Box 25007, Denver, CO 80225

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 Denver Office Reclamation Services and Applications Mission Support (DO RSAMS) - Reclamation Information Sharing Environment (RISE) is a web-based application that aggregates, stores, manages, publishes, and/or links to copies of mission-related data for access and use by internal (Reclamation) and external (non-Reclamation) users. It provides publicly accessible access to this mission-related data in

a single portal, using common machine-readable formats. The RISE user interface includes a data catalog, query interface, map interface, data visualization, web services, and data download. A website administration interface allows system administrators and content creators to add, change, and remove content from the user interface website. A data administration interface allows data owners and stewards to manage and maintain the mission-related data hosted or displayed through the user interface, including managing sharing permissions.

There is no sensitive data on the RISE website. RISE contains copies of Reclamation's mission-related data such as water, hydropower, environmental, infrastructure data, assets data, and associated metadata. Data consists of documents, time series data, geospatial data, tabular data, etc. RISE also contains system administration data (such as user account information). The RISE system helps fulfill Reclamation's responsibilities under the OPEN Government Data Act to make data assets available in open and machine-readable formats.

Users
RISE stakeholders/customers include internal and external users (e.g. Reclamation staff; partners from Federal, State, and local agencies; water and power users, researchers, media outlets, and the general public).

Location
The infrastructure, operations, and IT support for RISE is maintained by local general support system staff and the system is part of BOR General Support System (BOR GSS), located in the Denver Regional Office, Denver, Colorado. The RISE servers are located in the Denver datacenter in the Denver Federal Center, Building 53.

C. What is the legal authority?

Foundations for Evidence-Based Policymaking Act (Public Law 115-435), Title II, the "Open, Public, Electronic, and Necessary (OPEN) Government Data Act of 2018.").

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

E. Is this information system registered in the Governance, Risk and Compliance platform?

☒ Yes: UII - 010-000000299, Reclamation Information Sharing Environment (RISE) System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII	Describe
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)*
INTERIOR/DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), modification published 86 FR 50156 (September 7, 2021); and INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), modification published 86 FR 50156 (September 7, 2021), available at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Email Address
☒ Other: PII is collected in RISE as described below:

RISE "Contact Us" Form
The RISE system offers a "Contact Us" form for users (external or internal) to submit comments or questions. The form allows users the option to provide their name, email address, subject of their comment, and other information (e.g., affiliation, desired use of data from RISE).

Data Administration User Interface
The RISE system includes a form as part of the data management user interface that allows users with appropriate permissions (internal data stewards and administrators) to input basic metadata about datasets, including contact information for data owners, managers, and contacts (name, email address, and Active Directory status retrieved from DOI Enterprise Active Directory)

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

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

RISE "Contact Us" Form
Information is collected via a form on the RISE website.

Data Administration User Interface
Information is shared between RISE and DOI Enterprise Active Directory (EAD) (Name, email address, and AD status).

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

RISE "Contact Us" Form
RISE contact us form allows users (internal or external) to submit a comment or question to the RISE team. The form gives users the option to provide their name, email address, subject of their comment, and other information (e.g., affiliation, desired use of data from RISE). Name, email, and subject of the comment are used by the RISE team to respond to comments and provide occasional informational announcements about the system. Other information (e.g., user affiliation and desired use of RISE data) is used to understand types of users and desired uses of the system in order to inform system planning and future development.

Data Administration User Interface
The information collected through the Data Administration User Interface is used as metadata for datasets published through RISE. Some metadata (e.g., title, description, tags, theme, location, parameter) is displayed to users of the RISE website as part of dataset catalog search results. Contact information for data

owners, managers, and stewards (name, email address, and AD status) is not displayed on the RISE website, but it is used by RISE system administrators to contact appropriate personnel about user comments/questions, dataset issues, or system errors related to datasets.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe how the data will be used.*

RISE "Contact Us" Form
PII collected from the Contact Us form may be shared with specific RISE team members or other Reclamation staff to respond to questions, address comments, or provide support for use of RISE.

Names and email addresses will also be added to the RISE contact list, currently managed in Cision software, for the purpose of distributing announcements about the RISE system.

Data Administration User Interface
PII collected in the Data Administration User Interface will be used by RISE system administrators to contact appropriate personnel about user comments/questions, dataset issues, or system errors related to datasets.

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

If unusual findings need to be escalated, the CDM team will report findings to designated DOI officials (DOI-CIRC).

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

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

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

Contractor Systems Administrators (authorized employees only) review and analyze RISE audit records at least weekly for indications of inappropriate or unusual activity and reports findings to designated DOI officials.

☐ 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

RISE "Contact Us" Form
Providing PII is optional on the Contact Us form. https://data.usbr.gov/contact Therefore, visitors can choose not to provide PII. This is also stated in the Privacy Notice above the form. After a user's name and email address are added to the RISE email list, that user can unsubscribe from the list using a link in the email or by contacting the RISE team.

Data Administration User Interface
Individuals may identify themselves or others as Data Contacts, Managers, and Owners for specific datasets in the RISE system. After being identified as a Contact, Manager, or Owner, individuals may request to be removed from the assigned role.

☐ No

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.*

RISE "Contact Us" Form
The following privacy notice is displayed on the RISE "Contact Us" page:

IF YOU SEND US EMAIL
You may choose to provide us with personal information, as in e-mail with a comment or question. We use the information to improve our service to you or to respond to your request. Sometimes your email may be forwarded to other government employees who may be better able to help you. Except for authorized

law enforcement investigations, we do not share your e-mail with any other outside organizations.

Notice is provided through the publication of this PIA and system of records notices: INTERIOR/DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), modification published 86 FR 50156 (September 7, 2021); INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), modification published 86 FR 50156 (September 7, 2021).

☒ Other:

To logon to a Reclamation computer, a DOI Warning Banner appears which informs the users they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

RISE "Contact Us" Form
For users who have provided their email address, name, and other information about themselves or their comment, this data may be retrieved through a manual or automated process that queries the information from the DOI email system, a compilation of RISE contact form submissions, and/or the RISE email distribution list for use in a distributed mailing list or individual email.

Data Administration User Interface
For users who are identified as a Data Contact, Manager, and/or Owner for one or more RISE datasets, this data may be retrieved through a manual or automated process that queries the information from the RISE database.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

RISE "Contact Us" Form

Reports are not produced on individuals using data provided via the "Contact Us" form.

Data Administration User Interface
Reports on individuals may be produced to identify datasets for which an individual is assigned as a Data Contact, Manager, or Owner in order to verify that the correct person is assigned or to contact an individual associated with a particular dataset. Reports may also be produced to identify individuals with particular AD statuses (e.g. inactive AD accounts) to identify possible needs for changes to assignments.

☐ No

Section 3. Attributes of System Data

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

RISE "Contact Us" Form
It is the responsibility of the individual submitting the form to verify the accuracy of the information provided in the "Contact Us" form. RISE relies on the accuracy of the information provided by the individual.

Data Administration User Interface
All information on individuals assigned as Data Contacts, Managers, and Owners comes from the DOI Enterprise Active Directory system. Domain Admins check the information for accuracy at creation and updates.

B. How will data be checked for completeness?

RISE "Contact Us" Form
It is the responsibility of the individual to check the information provided in the "Contact Us" form for completeness. RISE relies on the completeness of the information provided by the individual.

Data Administration User Interface
All information on individuals assigned as Data Contacts, Managers, and Owners comes from the DOI Enterprise Active Directory system, and accuracy is verified

by that system. Domain Admins check the information for completeness at creation and updates.

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

RISE "Contact Us" Form
For public users, it is the users' responsibility to ensure their information is current when providing it in the "Contact Us" form.

Data Administration User Interface
All information on individuals assigned as Data Contacts, Managers, and Owners comes from the DOI Enterprise Active Directory system. Domain Admins check the information for currency at creation and updates.

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

Records in this system are maintained under Departmental Records Schedule (DRS) as follows: Information contained about water resources, hydro-power generation, water quality, and biological denizens, and other programmatic data are reference copies of records, and are thus considered "not records" in this system. These records do not have PII.

RISE "Contact Us" Form
The RISE "Contact Us" form is temporary. The retention of the form is transitory and destroyed when no longer needed.

Data Administration User Interface

Records on user activity are retained in accordance with DRS – Administrative schedule 1.4 A.1 – [0013] Short Term IT Records – System Maintenance and Use Records (DAA- 0048-2013-0001-0013). These records have a temporary disposition. Records are cut-off when obsolete and destroyed no later than 3 years after cut-off.

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

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 a limited privacy risk associated with the RISE system. Visitors to the RISE website may view and search publicly available data anonymously without providing PII. Users have the option to provide their email address and name via the RISE "Contact Us" form to be used to receive responses to comments and occasional email updates about RISE. This PII is stored in SharePoint files with access permissions limited to members of the RISE team and/or Reclamation's media contact management system (Cision) with access limited to specific RISE team members and Office of Communications staff. In the Data Administration User Interface, Reclamation personnel may be assigned as Data Contacts, Managers and/or Owners of datasets published in RISE, but no PII is made publicly available.

This PII is stored internally in the RISE database, and access to the information is monitored and controlled. All PII collected by RISE is non-sensitive. Users can decline to provide PII via the Contact Us form. Users assigned as Data Contacts, Managers and/or Owners may request that they be removed from the assigned role. RISE is housed on virtual servers hosted at the Bureau of Land Management (BLM) datacenter, a secured environment that houses the CMS and content delivery network operated by BLM. The CMS by which the website is published is accessed by BOR content authors using Active Directory Federation Services for authentication. Direct connection for administrators is done using a secured FIPS compliant virtual private network (VPN). The RISE CMS and its computer infrastructure employ software programs to monitor network traffic to identify unauthorized attempts to upload or change information or otherwise case damage. RISE uses HTTPS to ensure all communications between RISE and members of the public are encrypted and secure, and to protect the privacy and integrity of any

exchange of information. Encryption prevents the public information from being read or changed while in transit as well as interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data.

RISE has undergone a formal Assessment and Accreditation 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. RISE is rated as Moderate based on the type of data, and it requires the Moderate baseline of security and privacy controls to protect the confidentiality, integrity, and availability of the PII contained in the system.

There is a risk that data may be inappropriately accessed or used for unauthorized purposes. In an effort to protect the privacy of individuals, Reclamation collects only the minimal amount of user information to contact individuals and identify individuals associated with specific datasets.

RISE uses session cookies for technical purposes such as to enable better navigation through the site, or to allow users to customize their preferences for interacting with the site. Like many websites, usbr.gov uses "persistent cookie" technology. A persistent cookie is a small text file that the website places on the user's web browser so that it can gather anonymous summary demographic information and remember the user's browser when it is used to visit the site again later. These cookies uniquely identify a browser on a computer, but never a person. In other words, if the same person uses Chrome and Internet Explorer, two unique browsers cookies will be assigned, one for each browser, so that person will be counted as two different visitors because visits are based on browsers, not computers or persons. These persistent cookies fall under the category of “Tier 2 – multi-session without PII” as described by the Office of Management and Budget (OMB) Memorandum “Guidance on Online Use of Web Measurement and Customization Technologies”, dated, June 25, 2010. This tier encompasses any use of multi session web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies). The DOI Privacy Policy provides information on the use of cookies and how users may opt out and disable cookies in their browsers.

All DOI employees and contractors are required to complete privacy, security, and records management awareness training, as well as role-based training on an annual

basis and sign the DOI Rules of Behavior prior to accessing any system to include RISE. Security role-based training is also required for security personnel and officials with special roles and privileges.

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

RISE "Contact Us" Form
RISE system is designed to provide data to both internal and external users, and in turn respond to the changing needs of the user community. For the RISE team to communicate directly with customers, the storage of minimal user information is relevant and necessary.

Data Administration User Interface
For the RISE team to identify points of contact for specific datasets to contact appropriate personnel about user comments/questions, dataset issues, or system errors related to datasets, the use of minimal user information is relevant and necessary.

☐ 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 the 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.

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:* Database Administrator

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

RISE "Contact Us" Form

PII is stored in SharePoint files with access permissions limited to members of the RISE team and/or Reclamation's media contact management system (Cision) with access limited to specific RISE team members and Office of Communications staff.

Data Administration User Interface
PII is stored internally in the RISE database, access is limited to Reclamation personnel based on RISE user roles, and access to the information is monitored and controlled.

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:

Privacy Act contract clauses are included. The standard Privacy Act contract clauses as well as other clauses for the handling of Federal information are included in all contracts for this system.

☐ 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*

The RISE system performs routine audit logging of actions taken within the system. The system administrator and other IT security personnel can access the audit logs.

☐ No

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

For system administrators, usernames can be associated with any of the following events and are captured in the RISE audit logs: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Actions of public users are not monitored.

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

Reclamation complies with National Institute of Standards and Technology (NIST) and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration. The use of DOI and Reclamation IT systems is conducted in accordance with the appropriate DOI and Reclamation use policy.

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 Information System Owner oversees and manages the protection of agency information processed and stored in RISE. The RISE Information System Owner, Product Manager, IT Project Manager, and the Information System Security Officer (ISSO), in collaboration with the Reclamation Associate Privacy Officer, are responsible for ensuring adequate safeguards are implemented to protect individual privacy and addressing complaints in compliance with Federal laws and policies for the data managed, used, and stored in RISE.

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 RISE Information System Owner is responsible for 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 RISE Information System Owner, Product Manager, IT Project Manager, and ISSO are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of agency PII is reported to DOI-Computer Incident Response Center (CIRC), the DOI incident reporting portal, in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact on individuals, in consultation with the Reclamation Associate Privacy Officer.