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: Reclamation Information Sharing Environment (RISE)
Bureau/Office: Bureau of Reclamation
Date: July 23, 2020
Point of Contact:
Name: Regina Magno
Title: Reclamation 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 Reclamation Information Sharing Environment (RISE) system will aggregate, store, manage, publish, and/or link to copies of mission-related data for access and use by internal Bureau of Reclamation (Reclamation) and external (Non-Reclamation) users. It will provide access to this mission-related data in a single portal, using common machine-readable formats. The RISE user interface will include a data catalog, query interface, map interface, data visualization, web services, data download, and customized alerts for mission-related data. The RISE website does not contain any personally identifiable information. Visitors may view, search and download information anonymously, or may voluntarily elect to create a user account through the General Administration Services (GSA) Login.gov in order to save their searches and set alerts for updates to website content. There is no sensitive data on the RISE website, user accounts are provided for the user's convenience and to promote public outreach. Login.gov registers user accounts and authenticates RISE users who choose to register a Login.gov account to access hosted federal agencies' applications.

A website administration interface will allow system administrators and content creators to add, change, and remove content from the user interface website. A data administration interface will allow data owners and stewards to manage and maintain the mission-related data hosted or displayed through the user interface, including managing sharing permissions. The RISE system will help fulfill Reclamation's responsibilities under the OPEN Government Data Act to make data assets available in open and machine-readable formats. RISE is the replacement for the Reclamation Water Information System (RWIS). RWIS functionalities and data will be converted into RISE. The RWIS web portal will be retired after RISE is officially authorized to operate within the Reclamation production environment.

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: *Describe*

E. Is this information system registered in CSAM?

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

☒Yes: 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** *(Yes/No)*	**Describe** *If Yes, provide a description.*
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-08, DOI Social Networks covers interactions with the public; DOI-47, HSPD-12: Logical Security Files (Enterprise Access Controls Service/EACS) covers DOI network credentials.

Records in Login.gov are maintained by GSA under the GSA/TTS-1, Login.gov, system of records notice.

☐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: *Specify the PII collected.*

Usernames will be collected from Active Directory for Reclamation staff/contractors who need elevated privileges to support the RISE system with assigning roles and permissions. Users may provide additional information about themselves when they create their profiles. This information may include name, email address, organization type and interests. This information is visible to RISE administrators and is not visible to other members of the public. Visitors may provide their contact information when submitting comments in the Contact Us form, which will be used to communicate with the individual.

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*

Information is either shared between RISE and Login.gov (UUID) or between RISE and EAD (AD username). See section D below for further details.

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

For public users, the Login.gov Unique User ID (UUI) will be used as a username, which will allow them to save settings and preferences and get alerts. If Users desire to have their name associated with their profile, they will have to add that within the RISE application after they have established their account. Users will have the option of allowing their email addresses (private or corporate) and names (if it was added to their RISE profile) to be used to allow the RISE program to send out new feature notifications and occasional updates from the program. User successful and unsuccessful login activity will be logged. Visitors may provide their contact information when submitting comments in the Contact Us form, which will be used to communicate with the individual.

For DOI users, DOI username data will be extracted from integration with the DOI Enterprise Active Directory (EAD) system, which authenticates users on the DOI network. When a user logs in and navigates through the system their username will be captured in system audit logs. Audit logs provide a chronological record of information system activities, including records of system accesses and operations performed in a given period. In order to set up permissions within the application user names of individual users are associated with folders/groups that determine permission/access.

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.* The Reclamation Systems Administrators (authorized employees only) review the audit records at least weekly for indications of inappropriate or unusual activity and work with the Reclamation CDM team for security event management using Splunk.

☒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 Tribal, state or local agencies 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: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

RISE is a publicly accessible website that can be accessed without the requirement of creating an account. Users may visit the website to search and download information anonymously. If Users desire to have their name associated with their profile, they will have to add that information within the RISE application after they have established their account. Users will have the option of allowing their email addresses (private or corporate) and names (if it was added to their RISE profile) to be used to allow the RISE program to send out new feature notifications and occasional updates from the program. If public users elect to create an account, they will be directed to leverage the GSA Login.gov system and can review the privacy policy, system of record notice and privacy impact assessment. Links will be provided on the RISE application's About RISE web page to review this information.

Authorized users within the DOI network that access the information system will be leveraging Single Sign On / Security Assertion Markup Language (SSO/SAML) authentication and see a warning banner prompt that will allow them to decline continuing and providing their information to the system.

☐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.*

The following privacy notice is placed 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: DOI-08, DOI Social Networks published July 22, 2011; DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) published May 12, 2007.

GSA provides notice through the Login.gov privacy policy, Login.gov PIA published on August 15, 2018; and the GSA system of records notice GSA/TTS-1, Login.gov.

☒Other: *Describe each applicable format.*

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.).

For users that have elected to be contacted for specific instances and provided the information, their emails and names (if the user added their name to their RISE profile as names are not required) may be retrieved through a manual or automated process that queries their information for use in a distributed mailing list or individual email.

I. Will reports be produced on individuals?

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

Reports are not produced on individuals but on the actions of users. If actions show unusual/suspicious or malicious behavior the logs can correlate the actions taken in the system with a "User Name". Reports can be generated to include any of the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. Reports can also include the following web application specific events which can also be generated in the reports: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Only systems administrators and the information system owner will have access to the reports.

☐No

Section 3. Attributes of System Data

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

Usernames will be collected from Active Directory for Reclamation staff/contractors who need elevated privileges to support the RISE system with assigning roles and permissions.

General users will be required to set up accounts through Login.gov. The identity assurance level for RISE accounts created through Login.gov are categorized at IAL1. At IAL1, identity proofing is not required, therefore any names in credentials and assertions are assumed to be pseudonyms. IAL1 allows a partner agency to distinguish a user account based on the email address provided by the user and the Universally Unique Identification Number (UUID) assigned by Login.gov to that user. Each UUID is a 128-bit number.

B. How will data be checked for completeness?

Public user information is verified for completeness by the user when registering for Login.gov. Members of the public may also choose to provide RISE with personal information, as in e-mail with a comment or question. RISE relies on the completeness of the information provided by the individual. The RISE system authenticates internal users through Active Directory Federated Services (ADFS) for single sign-on.

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

For public users, it is the users' responsibility to ensure their information by updating their profile information. Internal user's information will be updated any time their role within the application changes and is maintained through the application account management policy.

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.

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 384 Departmental Manual 1.

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

There is a limited privacy risk for use of name and email address to communicate with and use of the RISE system. Visitors to the RISE website may view and search publicly available data anonymously without creating a user account or providing PII. Users will have the option of allowing their email addresses (private or corporate) and names (if it was added to their RISE profile) to be used to allow the RISE program to send out new feature notifications and occasional updates from the program. The information in the application is stored internally and access to the information is monitored. The PII identified is in the form of email addresses and other non-sensitive PII. All entries of PII are completely optional for the user.

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.

There is a risk that users may not receive adequate privacy notice. User accounts and identity authentication is handled by the GSA Login.gov for public users, and information is transferred over an encrypted tunnel to the application. Users are provided with a Login.gov privacy policy that includes a Privacy Act statement and may also view the GSA Login.gov privacy impact assessment and system of record notice for information on privacy implications. Login.gov user account information is maintained by GSA and is not shared with DOI.

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 create and manage user accounts and authenticate users and to contact individuals. RISE user accounts are properly managed, user access is authenticated and authorized, access is restricted to authorized personnel, and user accounts are disabled or deleted after defined periods of inactivity based on NIST guidelines. Additionally, elevated roles/privileges are assigned to approved users. Audit logs are used to track system activity. System Administrator assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

RISE uses session cookies for technical purposes such as to enable better navigation through the site, or to allow you to customize your preferences for interacting with the site. Like many websites, usbr.gov uses "persistent cookie" technology. A persistent cookie is a small text file that this website places on your web browser so that it can gather anonymous summary demographic information and remember your 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 browser 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 multisession 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: *Explanation*

The 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, or for users to create their own accounts on RISE to allow them to save information and queries of the data, the storage of minimal user information is practical 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 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

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 Administrators

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

Access is restricted to user's roles determined by the RISE Administrators. Access to data is restricted through permissions and access controls. System administrators have access based on a need to know and least privilege principle.

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?*

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. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events and will include the identity of users 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. Only authorized users with system administrator privileges have access to monitor user's activities in the system. RISE follows the NIST 800-53 controls and DOI security and privacy control standards for user access based on least privilege, ensuring that only authorized individuals are authorized to have access to system data.

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 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 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.