



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: Lower Colorado Basin Reclamation Services and Applications for Mission Support (LCB RSAMS)

Bureau/Office: Bureau of Reclamation/Lower Colorado Basin Regional Office

Date: February 11, 2022

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 Lower Colorado Basin Reclamation Services and Applications for Mission Support (LCB RSAMS) is a collection of Information Technology resources across the Lower Colorado Basin Region that provides mission-specific functions deemed to have significant impact on the Region's mission and business operations if the confidentiality,



integrity, or availability of these resources were compromised. Specifically, the parent LCB RSAMS contains a minor application (Work Plan Database (WPD)) which is a database that supports Region's water resource management.

Active Directory (AD) account information for user access is through Enterprise AD (EAD), which is assessed separately through the Department of the Interior's (DOI) Enterprise Hosted Infrastructure (EHI). The EHI privacy impact assessment (PIA) is available at <https://www.doi.gov/privacy/pia>. Services such as, encryption protection, virus/malware protection, system management, and vulnerability scanning are assessed separately through the BOR General Support System (BOR GSS) as these are Bureau-wide services.

This PIA is being conducted to document the privacy protections that are in place for the LCB RSAMS infrastructure. This PIA will be updated as the authorization boundary changes, or subsystems are added to address any privacy risks. Any subsystem that presents unique privacy risks will be assessed separately.

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); the E-Government Act of 2002 (Public Law 107-347), as amended; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

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 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 Codes: 010-000000299



Lower Colorado Basin Reclamation Services and Applications Mission Support
(LCB RSAMS) 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
Lower Colorado Basin Work Plan Database (LCB WPD)	Budget Formulation	Yes	Username are authenticated through Active Directory. A Separate PTA has been completed to address the use of Active Directory for authentication.

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)*

Active Directory records are covered by 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.

☐ 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



☒ Other: LCB RSAMS utilizes EAD, which collects username, password hash values, business contact information, official title, Personal Identification Verification (PIV) credential certificate information, and supervisor 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

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: Information from AD is user data that is provided upon creation of the account with DOI Access user credentials. EAD continuously updates data across the DOI Domain. When a user logs onto the system the 'username' is captured in system audit logs, which provide a chronological record of information system activities, including access and operations performed by a specific user and documented with a date and time stamp.

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

PII is used in the creation and administration of AD accounts for the purpose of authenticating individuals and managing user access to the DOI network and Reclamation's computing environment. EAD provides access control and user authentication services across the DOI Domain.

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



- ☒ Within the Bureau/Office: User information may be shared to support access management functions for the network and computing environment, including resetting passwords and authenticating the identity of users. System administrators perform reviews to ensure that all active user accounts are current employees with a need for access. In the event of an incident response investigation, it may be necessary to share the information with internal investigators.
- ☒ Other Bureaus/Offices: The LCB RSAMS is comprised of infrastructure components and any data within the system is limited to officials and users conducting official business. Data residing on the LCB RSAMS system will be shared with other DOI Bureaus and Offices for official purposes, including incident reporting, security monitoring events that may result in criminal investigations and only when given proper authorization through the correct channels within DOI and/or Reclamation.
- ☒ Other Federal Agencies: The HSPD-12 program is a government-wide requirement managed by the General Services Administration (GSA) 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. Some information may be shared with other Federal Agencies as authorized pursuant to the routine uses contained in DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.
- ☒ Tribal, State or Local Agencies: 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, authorized by law or under the Privacy Act.
- ☒ Contractor: User information may be shared to support application issues and maintenance.
- ☐ 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: User information is voluntarily provided by employees, originally created and obtained during new employee onboarding process for PIV credentials through various forms that contain Privacy Act Statements that include the Authority, Purpose, Routine Uses, and Disclosure. Users can consent during the onboarding process to provide their information for issuance of government credentials. If users decline to provide the required information upon employment, they will not be provided credentials or a domain user account to access the DOI network and information systems, which will impact



employment.

☐ 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: Users are provided a Privacy Act statement during new employee onboarding process for PIV credentials.

☒ Privacy Notice: Notice is provided through the publication of this PIA. Employees may also view the Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment (PIA) and the DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice for information on network user information is handled.

☒ Other
- Warning Banner

The following notice is provided by Reclamation's login banner to the network.

WARNING TO USERS OF THIS SYSTEM. THIS IS A NOTICE OF MONITORING OF THE DEPARTMENT OF THE INTERIOR (DOI) INFORMATION SYSTEMS.

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.

☐ None



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

Information is retrieved using EAD native tools that allow for the retrieval by employee name, username, workstation name and EAD group name.

I. Will reports be produced on individuals?

- ☒ Yes: LCB RSAMS can generate audit reports. Audit logs show username, date and time of system access, number of failed attempts and commands initiated. Audit logs may also record specific files accessed by the user if such logging is enabled. The System Administrator can provide audit logs and share them with other entities if an event needs investigation.

☐ No

Section 3. Attributes of System Data

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

Data is not collected from other sources.

B. How will data be checked for completeness?

Users are responsible for the completeness of the information provided in forms through the on-boarding process and other LCB RSAMS process. User information is obtained from AD and is updated through procedures managed by the EAD and cannot be changed at the LCB RSAMS level. LCB RSAMS forms have manual processes to ensure completeness of information provided by the user. Work related contact information attributes can be updated through a request from the employee.

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

System account administration work orders follow standard operating procedures which are updated as changes occur to the account management process. The procedure includes verifying that the current user accounts on the system are associated with active employees. User information that is obtained from the EAD is kept current through procedures managed by DOI. Following the Continuous Diagnostic and Mitigation requirements, accounts are reviewed monthly. Employees can update their work-related contact information through various means including the My Account site in DOI's Bison Connect email system.



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

Records on user activity are retained in accordance with Department Records Schedule (DRS) – 1, 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?

Once user accounts are terminated in the system, the records are removed in accordance with the DRS and other applicable bureau/office records retention schedules. Reports are not generated. Procedures for disposition of the data stored in individual applications will vary by application. When a user account is disabled or terminated in the EAD, all access will be denied since the user will no longer have the ability to log onto or authenticate to the network. The EAD 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 LCB RSAMS systems are explicitly denied and all attempts to gain access are logged.

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

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

There is minimal privacy risk to the employees related to user access information contained in AD. The PII contained in AD and includes employee name, username, work email address, work phone number, duty station address, and official title. This information is not considered sensitive. Application permissions and access controls are in place to limit application access to only those authorized individuals with a need to know the information to perform official functions.

LCB RSAMS is to undergo a formal Assessment and Authorization to be granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. LCB RSAMS is rated as a FISMA low 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.



LCB RSAMS has developed a System Security and Privacy 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 LCB RSAMS to identify and mitigate vulnerabilities found. Security and privacy awareness training is required for all Reclamation 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 and Privacy role-based training is also required for security personnel and officials with special roles and privileges.

Reclamation 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 LCB RSAMS. The use of Reclamation IT systems, including LCB RSAMS, is conducted in accordance with the appropriate DOI 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 immediately reported to IT Security.

The system follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user.

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: User information is required for user access control and management to Protect the DOI network and information systems.

☐ 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 as LCB RSAMS does not generate new data.

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: Auditors and/or DOI Assessment Team may access the system at least annually.

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



Access to AD is restricted to System Administrators who have a need to know to perform their duties. Regular users only have access to their information and applications needed to perform their duties. Access is granted on a least privilege access basis.

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?*

☒ 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: All user activity is audited as part of the security monitoring and management of user accounts. Usernames can be associated with any of the following events in the audit logs: account management events, object access, privilege functions, process tracking, system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes and permission changes.

☐ No

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

The auditing of user activity includes, but it not limited to, successful and unsuccessful account logon events, username, date/time, account management events, object access, policy change, privilege functions, process tracking and system events.

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

Reclamation 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 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, including LCB RSAMS, 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. LCB RSAMS implements the NIST 800-53 security controls and DOI security and privacy control standards for user access based on least privilege, ensuring that only authorized individuals have access to system.

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 LCB Regional Director serves as the LCB RSAMS Information System Owner and the official responsible for oversight and management of the LCB RSAMS security and privacy controls. The DOI Information System Owner for EAD, the Logical Security Files Privacy Act System Manager, the Information System Owner and Information System Security Officer, in collaboration with the Regional Privacy Officer and the Reclamation Associate Privacy Officer, are responsible for ensuring adequate safeguards are implemented to protect individual privacy at the appropriate levels in compliance with Federal laws and policies, and for addressing Privacy Act requests and complaints in consultation with DOI Privacy Officials. Program officials and users are responsible for protecting PII within their area of responsibility and meeting requirements under the Privacy Act and Federal law and policy.

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 LCB RSAMS Information System Owner is responsible for oversight and management of the LCB RSAMS security and privacy controls, and for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and EAD Information System Owner are responsible for reporting any loss, compromise, unauthorized access, or disclosure of PII to DOI-CIRC within one hour of discovery in accordance with Federal policy and established procedures and appropriate remedial activities are taken to mitigate any impact on individuals, in coordination with



Reclamation's Associate Privacy Officer. Program officials and users are responsible for reporting any compromise of PII in accordance with Federal and DOI policy.



Section 5. Review and Approval

Information System Owner

Name: Jacklynn L. Gould

Title: Lower Colorado Basin Region Regional Director

Bureau/Office: Bureau of Reclamation/Lower Colorado Basin Regional Office

Phone: 702-293-8409

Email: jgould@usbr.gov

Signature: **JACKLYNN
GOULD**

Digitally signed by
JACKLYNN GOULD
Date: 2022.02.01
13:50:56 -05'00'

Information System Security Officer

Name: Monique Braun

Title: Regional Information System Security Manager

Bureau/Office: Bureau of Reclamation/Yuma Area Office

Phone: 928-343-8263

Email: mbraun@usbr.gov

Signature: **MONIQUE
BRAUN**

Digitally signed by
MONIQUE BRAUN
Date: 2022.01.26
11:55:03 -07'00'

Privacy Officer

Name: Regina Magno

Title: Associate Privacy Officer

Bureau/Office: Bureau of Reclamation/Denver Office

Phone: 303-445-3326

Email: rmagno@usbr.gov

Signature: **REGINA
MAGNO**

Digitally signed by
REGINA MAGNO
Date: 2022.01.24
13:26:47 -07'00'

Reviewing Official

Name: Teri Barnett

Title: Departmental Privacy Officer

Bureau/Office: Office of the Secretary/Office of the Chief Information Officer

Phone: 202-208-1943

Email: ngoc_thuy_barnett@ios.doi.gov

Signature: