



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: Lower Colorado Basin Dams Industrial Control Systems - Electronic Access Control and Surveillance System (LCB Dams ICS - EACSS)

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

Date: August 27, 2024

Point of Contact:

Name: Regina Magno

Title: Associate Privacy Officer

Email: privacy@usbr.gov

Phone: (303) 445-3326

Address: P.O. Box 25007 (84-21000), Denver, CO 80225-0007

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:

B. What is the purpose of the system?

The Lower Colorado Basin Dams Internal Control System Electronic Access Control and Surveillance System (LCB Dams ICS - EACSS) supports the Lower Colorado Basin Dams Office's ability to carry out critical security services aimed at protecting the



public and Reclamation employees through physical access control and video surveillance of Hoover, Parker, and Davis Dams.

The LCB Dams ICS - EACSS is a physical protection system consisting of technical capabilities designed to provide an integrated method of detection and response to alarms, threats, and other adversarial actors and activities, with an overarching purpose to provide access control and monitoring to perimeters with the facility that are either sensitive or secure. Its technical capabilities include electronic access control (PIV cards), alarm sensors, and video surveillance. This deployment does not interconnect with any other information system.

C. What is the legal authority?

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, section 5113); E-Government Act (Pub. L. 104-347, section 203); Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521); Government Paperwork Elimination Act (44 U.S.C. § 3504); Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, Section 3001 (50 U.S.C. 435b); Executive Order 9397; Executive Order 12968; Federal Property Regulations, July 2002; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

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 Governance, Risk and Compliance platform?

- ☒ Yes: 010-000000294, EACSS System Security 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:

INTERIOR/DOI-46, Physical Security Access Files, 85 FR 3406 (January 21, 2020);
Final Rule for Privacy Act Exemptions, 86 FR 49927 (September 7, 2021).

☐ No

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

☐ Yes

☒ No

Section 2. Summary of System Data

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

☒ Name

☒ Other: The LCB Dams ICS – EACSS system contains information on individuals that require regular, ongoing access to Hoover, Parker, or Davis dams, including employees, contractors, students, and interns. Visitor name and signature are collected as part of the visitor register. Video surveillance is used within the LCB Dams ICS - EACSS to monitor and detect unauthorized access to Hoover, Parker, or Davis dams. The only PII related aspect would be images used for manual facial recognition and identification and only used for incident-based scenarios of unauthorized access to the facilities including predetermined restricted areas.

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:

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

PII collected and maintained in LCB Dams ICS - EACSS is used to ensure only authorized employees and contractors with proper identification are permitted entry into Hoover, Parker, and/or Davis dams.

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

- ☒ Within the Bureau/Office:

Reclamation Systems Administrators and IT Security personnel (authorized employees only) manage user access, review, and analyze user account information (name, username, login dates, access attempts, etc.) against operating system and security events when providing help desk support, and report inappropriate or unusual activity to designated DOI officials. Security office personnel, system administrators, and contracted security guard staff at the Hoover, Davis, and Parker dam facilities, as well as the ICS and PSP (Physical Security Perimeter) that resides within the Hoover, Davis, and Parker dam facilities, have different defined levels of access to the data within the system, depending on their access rights. Security office personnel and security guard staff have 24/7 view only access to the data, this includes video footage and proximity card logs. Security office personnel and security guard staff are given this access for the purposes of providing a monitoring system with the overarching and goal of providing a robust, responsive, and 24/7 site wide physical security program that helps ensure the reliability and safety of the facility. System administrators located at Hoover, Davis, and Parker dams are the only individuals that have 24/7 read (view), write, and export access to the data that resides within the EACSS system including all forms of PII data that



resides on the system. System administrators are given this level of access to maintain, repair, and patch vulnerabilities, which helps to ensure that the PSP remains a reliable tool for the Security office personnel and security guard staff to provide the comprehensive security program that the Hoover, Davis, and Parker dam facilities need.

☒ Other Bureaus/Offices

Data residing on the EACSS system will be utilized by other DOI Bureaus and Offices only for criminal investigation purposes, and only when given proper authorization through the correct channels within the DOI and/or Reclamation Approval.

☒ Other Federal Agencies

Data may be shared with other Federal agencies, such as the Federal Bureau of Investigation or Department of Homeland Security if requested for investigative purposes due to criminal activity and only with proper DOI and/or Reclamation approval. The Bureau of Reclamation may share information with external agencies and organizations as authorized by the Privacy Act and outlined in the routine uses section of the published INTERIOR/DOI-46, Physical Security Access Files system of records notice.

☒ Tribal, State or Local Agencies

The Bureau of Reclamation may share information with Tribal, State or Local Agencies as authorized by the Privacy Act and outlined in the routine uses section of the published INTERIOR/DOI-46, Physical Security Access Files system of records notice, or when necessary for investigative purposes due to criminal activity and only with proper DOI and/or Reclamation approval.

☒ Contractor

Davis and Parker Dam security officers are contracted to ensure the reliability and safety of the facility using checkpoints, patrolling, and monitoring surveillance which enables them to apply the appropriate security response to any incident. Real-time video monitoring is defined with having the ability to rewind/fast forward live feeds from the surveillance system. Data access is read/view only permissions for the security officers on-duty and on a need-to-know basis.

☐ Other Third Party Sources

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 and contractors when requesting access to the Hoover, Davis, and Parker dam facilities. For individuals to report to their duty stations, basic information is required for granting the appropriate permissions while maintaining the integrity of security of the work site. If users decline to provide the requested information they will be denied access to the facility and will be unable to work at this location.

☐ No

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement:

A sign is posted in the visitor center letting individuals know that the facility is under video surveillance.

A Privacy Notice is provided to individuals through a posted sign at the entrance to the facility or displayed on monitors within the facility, and copies will be made available upon request. The notice includes legal authorities for collecting information, the purpose of the collection and uses of the information, how and to whom it is shared outside of the Department, and how the provision of information is voluntary and that visitors may decline to provide information and how that may prevent them from entering the facility.

☒ Privacy Notice:

Notice is also provided through the publication of this privacy impact assessment and the INTERIOR/DOI-46 Physical Security Access Files system of records notice.

☐ Other:

☐ None

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

Records may be retrieved by employee name; image; organization/office of assignment; date, time or location of entry or exit; or proximity card number.

I. Will reports be produced on individuals?



☒ Yes:

LCB Dams ICS - EACSS has limited reporting capabilities. Reports may be generated by the system administration upon request by Reclamation officials in response to security breach investigations. Reports on individuals will include name and time and location of access.

☐ No

Section 3. Attributes of System Data

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

It is the responsibility of the individual to verify the accuracy of the information collected.

B. How will data be checked for completeness?

All initial collection of information is obtained from the employee/contractor. It is the responsibility of the individual to verify the data is complete.

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

Data will be verified by comparing it with information in Reclamation Active Directory which provides an updated listing of active Reclamation employees. Data is also verified through email from HR notifications of terminations and transfers.

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

LCB Dams ICS - EACSS records are retained in accordance with the Departmental Records Schedule (DRS) 1.1.01.10, "Administrative - Short-term" which has been approved by the National Archives and Records Administration (NARA) (DAA -0048-2013-0001). LCB Dams ICS - EACSS records are cutoff at the end of the fiscal year and destroyed 3 years after cutoff.

Records schedules related to security violations or investigations that are referred to administrative or law enforcement organizations may vary depending on the subject matter, legal requirements and Departmental policy.

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). The disposition is Temporary. Cut off when superseded or obsolete. See records manual for specific criteria that may determine when a record is obsolete or superseded. Destroy no later than 3 years after cut-off. For user activity records, once user accounts are terminated in the system the records are removed in accordance with the DRS records retention schedule.

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 are risks to the privacy of individuals due to the volume of sensitive PII contained in LCB Dams ICS - EACSS. Video surveillance recordings are not associated with specific individuals and are not considered a record until an event or incident has occurred. At that point the footage will be copied over, associated with an investigation, and provided to the appropriate organization. Video data is retained for a maximum of up to 90 days on the LCB Dams ICS - EACSS system itself and no backups of the video files are created. When video footage is provided to external organizations, it is encrypted and the provision is authorized and documented.

LCB Dams ICS - EACSS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. LCB Dams ICS - EACSS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system. The data collected and maintained is limited to only the minimal amount of data needed for identification purposes in alignment with the purpose of an identity management system. The collection, use, retention, processing, and destruction of users’ information provided within the LCB Dams ICS - EACSS system is intended to maintain the integrity of the user’s information during the information lifecycle. Efforts are made in protecting the information so that access is limited to only system managers needing the data. The greatest risks identified in the lifecycle process are at the beginning and the end where paper copies are being used. The system itself is safeguarded by being isolated from all other systems and is inaccessible from outside access connection points. Only authorized individuals have access to the LCB Dams ICS - EACSS system.



The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail will include the identity of each user 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, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The LCB Dams ICS – EACSS 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. Reclamation employees and contractors are required to complete the security and privacy awareness training and sign the DOI Rules of Behavior. LCB Dams ICS - EACSS users and administrators are also required to sign an LCB Dams ICS - EACSS-specific Rules of Behavior.

All user information is captured in the audit logs and the system is protected by giving access only to valid, authorized personnel. This information is not shared outside of Reclamation as the system is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When the system reaches end of life the equipment and/or media that contains user information and audit logs will be retained in accordance with the records retention schedule for IT systems.

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:

The use of the data is relevant and necessary to physically identify individuals for facility access purposes and ensure the security of Reclamation personnel and facilities. The data collected and stored has intentionally been limited. Only the minimal amount of data needed for identification purposes is maintained and used by the system.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes

☒ No



C. Will the new data be placed in the individual's record?

☐ Yes

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes

☒ No

E. How will the new data be verified for relevance and accuracy?

LCB Dams ICS - EACSS does not derive new data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ 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: Security guard staff at Hoover, Parker, and Davis dams will have access to the data in the system for the purpose of verifying the identity of individuals who are authorized to enter the facilities but do not have their identification credentials with them. System Administrators and IT Security personnel will have access to the data in the system for maintenance purposes and for verifying individuals have the correct physical access rights.

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



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.

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

☒ No

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

☒ Yes.

LCB Dams ICS - EACSS is an identity management system and can identify individuals and monitor them entering and leaving the Hoover, Parker, and Davis dam facilities for physical security purposes.

☐ No

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

LCB Dams ICS - EACSS identifies authorized individuals upon entry and exit of the Hoover, Parker, and Davis dam facilities. Video surveillance also captures images of persons entering and leaving the facilities. Audit trails of activity are maintained to reconstruct security relevant events and include the identity of each user 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.



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 are 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' system administrator privileges have access to monitor user's activities in the system. LCB Dams ICS - EACSS 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: All visitors to the Hoover, Davis, and Parker dam facilities must be always escorted. Only those people with authorized unescorted access are allowed into restricted areas, otherwise known as physical security perimeters, where the data resides. The process for gaining this access is more stringent and provides another layer of security for the facility.

(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. System permissions that follow the concept of least privilege. The LCB Dams ICS - EACSS system is isolated from all other DOI and Reclamation systems, and access to the system requires physical presence at a terminal location, no VPN controls are used within the system.

(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: Designated authorizing officials for authorizing access to the system. Video data is retained for a maximum of up to 90 days on the LCB Dams ICS - EACSS system itself and no backups of the video files are created. When video footage is provided to external organizations, it is encrypted and the provision is authorized and documented.

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 Lower Colorado Regional Director serves as the LCB Dams ICS - EACSS Information System Owner and the official responsible for oversight and management of the security and privacy controls for the system. The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies for the data managed and stored in LCB Dams ICS - EACSS in consultation with the Reclamation Associate Privacy Officer.



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

The LCB Dams ICS - EACSS Information System Owner is responsible for oversight And management of the LCB Dams ICS - EACSS security and privacy controls, and for ensuring to the greatest possible extent the data is properly managed and all access to the data has been granted in a secure and auditable manner. The Information System Owner is also responsible for reporting any loss, compromise, or unauthorized access to the system or data is reported to the DOI Computer Incident Response Center within one hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any potential compromise.



Section 5. Review and Approval

Information System Owner

Name: Jacklyn L. Gould

Title: 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: 2024.07.30
09:37:30 -07'00'

Information System Security Officer

Name: Phillip Parada

Title: IT Specialist (Infosec)

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

Phone: (702) 494-2172

Email: pparada@usbr.gov

Signature: PHILLIP PARADA

Digitally signed by
PHILLIP PARADA
Date: 2024.07.30
08:15:04 -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: 2024.07.29
10:45:01 -06'00'

Reviewing Official

Name: Teri Barnett

Title: Departmental Privacy Officer

Bureau/Office: Department of the Interior/Office of the Chief Information Officer

Phone: (202) 208-1943

Email: ngoc_thuy_barnett@ios.doi.gov

Signature: