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: BOR Cloud Application Resource System (B-CARS)
Bureau/Office: Bureau of Reclamation/Information Technology Services Division
Date: November 8, 2024
Point of Contact:
Name: Regina Magno
Title: Associate Privacy Officer
Email: privacy@usbr.gov
Phone: 303-445-3326
Address: PO Bx 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

B. What is the purpose of the system?

B-CARS is the Infrastructure-as-a-Service(IaaS) cloud enterprise infrastructure using the Department of the Interior/Office of the Chief Information Office (DOI-OCIO) managed Azure Tenant Cloud Computing Environment. This environment provides a set of Information Technology (IT) resources across Reclamation. B-CARS is the cloud IT General Application Support System for Reclamation, supporting mission-specific functions, activities, and user generated data such as

planning, environmental programs, and office automation and support functions for water and hydroelectric power management objectives.

Cloud computing offers Reclamation unmatched flexibility in both usage policies and scalability. The short-term goal is to provide a platform that will allow adjustment of resources to match workload. The long-term goal is to save time, money, and manpower by having a scalable platform. The cloud is tailored to meet requirements in real time, mitigate the possibility of overspending to meet needs, and position Reclamation to have resources at its disposal when needed, and curb unnecessary infrastructure expenditures.

Active Directory (AD) account information for user access is through the DOI Enterprise AD, which is assessed separately through the DOI Enterprise Hosted Infrastructure (EHI). EHI's 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 this PIA as these are Bureau-wide services.

The user community accesses several services which may contain personally identifiable information (PII), however it is the responsibility of the application, data owner, or individual to protect the information and meet requirements under the Privacy Act and Federal law and policy. These services include office automation software such as Microsoft Office, Adobe products, BisonConnect, Geographical Information System (GIS), and DOI's applications which support Human Resources, Payroll, Finance, Personnel Security, and Acquisitions. The use of these services has been assessed separately in PIAs conducted at the Department and BOR levels and are outside the scope of this PIA.

This PIA is being conducted to document the privacy protections that are in place for the B-CARS infrastructure. Privacy risks for the hosted applications within the cloud will be assessed separately.

C. What is the legal authority?

Departmental Regulations (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 Governance, Risk and Compliance platform?

☒ Yes: UII Code: 101-000002502/ B-CARS 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: Active Directory records are covered by 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 program and user activities that may be subject to the Privacy Act are covered by various Department-wide SORNs which are found at https:\\www.doi.gov/privacy/sorn

☐ 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: Username. B-CARS utilizes Enterprise Active Directory (EAD) through the Enterprise Hosted Infrastructure (EHI). EAD collects username, password hash values, workstation name, business contact information, official title, Personal Identification Verification (PIV) credential certificate information, and supervisor name. In addition, all users are required to fill out security questions and answers to authenticate user identity and to assign access permissions. Due to the nature of the B-CARS, there is a potential for PII to be contained within the environment as program officials and users of this system may create, collect, store, process or maintain PII during business. This PII may include but is not limited to, names, email addresses, telephone numbers, SSNs, dates of birth, financial information, employment history, education background, and other information related to a specific mission purpose.

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 *Describe:*
Information from AD includes user data provided by EHI upon creation of the account with DOIAccess. AD continuously updates data across the DOI Domain.
☒ Other: Program officials and users of this system may access other systems or utilize various methods to create, collect, store, process or maintain PII during their daily duties and business functions.

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

PII is used in the creation and administration of AD user accounts for the purpose of authenticating individuals and managing user access to the DOI network and Reclamation computing environment. EHI provides access control and user authentication services across the DOI Domain. Security questions and answers are maintained in this system to authenticate user identity for password reset requests.

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 with Reclamation system administrators to support access management functions for the network and computing environment, including resetting passwords and authenticating the identity of users.

☒ Other Bureaus/Offices: B-CARS is comprised of infrastructure components and any data within the system is limited to user access information and data of program officials and users conducting official business. Data residing on B-CARS will be shared with other DOI Bureaus and Offices for official purposes, including incident reporting, security monitoring or criminal investigation purposes, and only when given proper authorization through the correct channels within the 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 Identity Verification Identity Management System. DOI user network access records are maintained under INTERIOR/DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice and may be shared with other Federal Agencies as authorized pursuant to the routine uses in the notice. These notices may be viewed at https://www.doi.gov/privacy/sorn.

☒ 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 INTERIOR/DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

☐ Contractor

☐ 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 in order to obtain access and authenticate to the DOI network and information systems. Users consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment, they will not be provided a user account to access the DOI network and information systems, which will impact employment.

☐ No

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

☒ Privacy Act Statement: User information is originally created and obtained during new employee onboarding process for PIV credentials, through various forms, including OF 306 and SF-85P, which contain Privacy Act Statements that include the Authority, Purpose, Routine Uses, and Disclosure.

☒ Privacy Notice: Notice is provided through the publication of this PIA. Employees may also view the EHI PIA and the INTERIOR/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

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.).

User AD information is retrieved by name, username, workstation name, and AD group names. This is typically done to reset passwords, change permissions, transfer/move accounts, and add/remove workstations.

I. Will reports be produced on individuals?

☒ Yes: Automated scheduled and ad hoc reports may be generated to audit user activity and determine accounts which need to be disabled due to employee separation. Data will include name, username, activity date/time, location and applications accessed.

☐ No

Section 3. Attributes of System Data

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

Users are responsible for the accuracy of the information provided in the forms through the on-boarding process and other Reclamation processes. B-CARS Forms have manual processes to ensure accuracy of information provided by the user.

B. How will data be checked for completeness?

Users are responsible for the completeness of the information provided in the forms through the on-boarding process and other Reclamation processes. User information is obtained from AD and is updated through procedures managed by the EAD and cannot be changed at the B-CARS level. B-CARS 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).

User information that is obtained from the EAD is kept current through procedures managed by

DOI. B-CARS forms collect information directly from users, so it is the responsibility of the user to provide current information. Employees can update their work-related contact information through various means including the My Account site in DOI's BisonConnect 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.

Due to the nature of B-CARS, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area.

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. When a user account is disabled or terminated, all access will be denied since the user will no longer have the ability to log onto or authenticate to the network. User accounts 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 information systems are explicitly denied and all attempts to gain access are logged.

Due to the nature of B-CARS, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area.

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

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 general user access information contained in AD. The PII contained in AD includes employee name, username, work email address, work phone number, duty station address, and official title. This information is not considered sensitive. System permissions and access controls are in place to limit system access to only those authorized individuals with a need to know the information to perform official functions. There is an increased risk to privacy due to the nature of the B-CARS and the potential for significant amounts of PII to be contained within the environment through the collection and processing of PII by program officials and users of this system while conducting official business.

There is a risk of unauthorized access or disclosure or that PII may be used for an unauthorized purpose. B-CARS has developed System Security and Privacy Plans 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 the B-CARS to identify and mitigate any 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 any B-CARS equipment. The use of Reclamation IT systems, including B-CARS, 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.

There is a risk the data may be stored for longer than necessary in B-CARS. Files should only be maintained in accordance with the 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.

There is a risk that individuals may not receive adequate notice on how their data will be used or shared. Notice is also provided through publication of this PIA and the INTERIOR/DOI- 47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records

notice. All users are presented with a warning banner (Reclamation disclaimer) when logging on to B-CARS that informs them they are accessing a Reclamation system, that they are subject to being monitored, and there is no expectation of privacy during use of the system. Any additional notice to individuals required by law and policy for specific sharing of records that contain PII with other organizations is the responsibility of the customer who is the data owner.

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: B-CARS is a cloud computing environment that provides IT resources across Reclamation to support mission-specific functions, activities, and user generated data such as planning, environmental programs, and office automation and support functions for water and hydroelectric power management objectives.

Data collected is relevant to perform functions of B-CARS and to support Reclamation's missions.

☐ 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?

Not applicable. B-CARS does not derive new data on individuals

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

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

Contractor's, system administrators, and auditors are granted access in accordance with mission function. B-CARS uses the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following FISMA, NIST guidelines, and DOI security and privacy policies.

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

☐ 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: B-CARS is IaaS using DOI-OCIO managed Azure Tenant Cloud Computing Environment. Azure has tools and technologies within their environment that DOI has not previously employed.

☐ 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 and can be reviewed by Enterprise and Domain Administrators, and Information Assurance personnel.

☐ 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, logon/logoff information, username, workstation name, IP address, date/time of activity, and application and/or website being accessed.

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

Access to administrative functions is strictly controlled to Enterprise and Domain Administrators. In addition, audit logging information is restricted to System Administrators and Information Assurance personnel. Audit features monitor user activities including logon/logoff information, username, workstation name, IP address, date/time of activity, and application and/or website being accessed to prevent unauthorized system access and 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 with system administrator privileges have access to monitor user's activities in the system. B-CARS 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 the 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

(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

(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

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 IT Services Division Manager serves as the B-CARS Information System Owner and the official responsible for oversight and management of the security and privacy controls for B-CARS and any FISMA "children" systems. The B-CARS Information System Owner and Information System Security Officer (ISSO), in collaboration with Senior Management and 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 on B-CARS.

The DOI Information System Owner for EHI and the Logical Security Files Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in EHI, and for addressing Privacy Act requests and complaints in consultation with DOI Privacy Officials. Program officials and users are responsible for protecting PII 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 B-CARS Information System Owner is responsible for daily operational 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 B-CARS Information System Owner and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC, the DOI incident reporting portal, in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in collaboration with the Reclamation Associate Privacy Officer.

As B-CARS utilizes EAD, which contains PII, the EHI Information System Owner is responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures. 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: Patrick McFall
Title: IT Services Division Manager
Bureau/Office: Bureau of Reclamation/Denver Office
Phone: 303-445-2271 Email: pmcfall@usbr.gov

Signature: PATRICK MCFALL Digitally signed by PATRICK MCFALL Date: 2024.10.12 10:35:19 -06'00'

Information System Security Officer
Name: Samuel Kankam
Title: Information System Security Officer
Bureau/Office: Bureau of Reclamation/Denver Office
Phone: 571-405-9382 Email: skankam@usbr.gov

Signature: SAMUEL KANKAM (Affiliate) Digitally signed by SAMUEL KANKAM (Affiliate) Date: 2024.10.15 08:06:27 -04'00'

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: 2024.09.05 09:44:29 -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: Teri Barnett Digitally signed by NGOC THUY BARNETT Date: 2024.11.08 14:03:02 -05'00'