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: Budget and Review System (BARS)
Bureau/Office: Bureau of Reclamation
Date: 3/14/2017
Point of Contact:
Name: Marie Hughes-Brown
Title: Assistant Director
Email: MHughesBrown@usbr.gov
Phone: 202-513-0518
Address: 1849 C Street, NW, Washington, DC 20240

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 Department of the Interior (DOI), Bureau of Reclamation (BOR) developed the Budget and Reporting System (BARS) as an automated tool to manage BOR budget execution processes and generate associated reports. The BARS tool will be used for allotting and tracking appropriation, funds control, and allowing for budget line (project) execution tracking using publicly available data. The Office of Program and Budget (P&B) is the BOR headquarters budget office and is required to provide information/status of funds regarding budget allotments, continuing resolution funding, sequestration funding, etc., to Regional Offices, HQ Offices and other internal and external BOR entities, Congress and the Office of Management and Budget (OMB).

BARS analyzes financial data obtained from the Financial and Business Management System (FBMS), the Department-wide financial management system, but is not connected to FBMS. Any data added to BARS will come from a Secure File Transfer Protocol (sFTP) site where there is no connection to any other systems. The purpose of BARS is to perform budget and funding functions and it is not intended for the collection personally identifiable information (PII).

BARS will:

- Validate that funds transfer requests can be approved by calculating available fund balances against business rules;
- Help the Reclamation business user derive sub allotment levels based up historic data, current continuing resolutions, rescissions, etc. that will be approved by the Regions and eventually submitted for entry into FBMS; and
- Provide reports such as the status of funds, quarterly funds transfers, and ad hoc reporting based upon office needs.

DOI and BOR have contracted with the International Business Machines (IBM) under the Federal Cloud Hosting Services (FCHS) indefinite delivery, indefinite quantity (IDIQ) to build and deliver BARS. BARS is a commercial-off-the-shelf (COTS) product that has been designated as a Cloud “Software as a Service” (SaaS), and will be hosted by SoftLayer Federal Cloud (SFC). SFC is a FedRAMP approved Infrastructure as a Service (IaaS) and has an Authorization to Operate (ATO) from DOI.

C. What is the legal authority?

- The Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521) requires federal agencies to minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information.
- 31 U.S.C. 331, Reports
- 31 U.S.C. 3513, Financial Reporting and Accounting System
- Federal Financial Assistance Management Improvement Act of 1999 (Public Law 106-107)

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?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000002323, The Budget and Review System (BARS) for the Department of Interior, Bureau of Reclamation

☐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.*
None	**None**	No	**N/A**

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐Yes: *List Privacy Act SORN Identifier(s)*
☒ 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
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Credit Card Number
☐ Law Enforcement
☐ Education Information
☐ Emergency Contact
☐ Driver's License
☐ Social Security Number (SSN)
☐ Personal Cell Telephone Number
☐ Tribal or Other ID Number
☐ Personal Email Address
☐ Mother's Maiden Name
☐ Home Telephone Number
☐ Child or Dependent Information
☐ Employment Information
☐ Military Status/Service
☐ Mailing/Home Address
☐ Race/Ethnicity

☒ Other: *Specify the PII collected.* Usernames are collected from users who logon and access the BARS system which allows BOR to authenticate users and manage permissions. These usernames are authenticated through the DOI Enterprise Active Directory (EAD).

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* The user's name and username data is extracted from integration with the EAD system, which authenticates users on the network. When a user logs in and

navigates through the system their “user name” and name 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 names of individual users are associated with folders/groups that determine permission/access.

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

Usernames are collected in the automated audit logs that provide a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant action from inception to final result. Names of individuals are associated with folders/groups that determine access/permissions within the application.

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

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

☐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.*

BARS contractor Systems Administrators (authorized employees only) review and analyze BARS 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.*

BARS users see a login banner when entering the system and must acknowledge and consent to having any personal information placed or sent over the system monitored and that there is no expectation of privacy before logging into BARS. Individuals can decide not to ask for access to the BARS application.

☐ 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.*

☒ Other: *Describe each applicable format.*

Before entering their username to log in to BARS, individuals are notified via a login banner that any information on the system can be monitored, recorded, copied and used for authorized purposes. Users can decline to login if they do not want their username recorded. Below is the BOR Warning Banner:

WARNING TO USERS OF THIS SYSTEM
This computer system, including all related equipment, networks, and network devices (including Internet access) is provided by the Department of 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.).

Logging of all actions occurs within the SFC platform. The following events are captured in the logs and can be used to retrieve information: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. Web applications specific events include: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. These events are analyzed by QRadar to identify potential issues. In the event an after-the-fact investigation is required, QRadar could provide automated analysis and Security Operations Center (SOC) personnel can provide manual review of all actions taken.

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?

BARS does not collect data from sources outside of the DOI. The user will enter their “user name” and password to access the application. This is authenticated through the EAD system.

B. How will data be checked for completeness?

The DOI EAD system will authenticate the user's "username" and credentials when the user logs into the Reclamation network, and these usernames and credentials are kept current by the EAD system.

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

BARS users must have valid and authorized DOI EAD account before they can log into the virtual private network and before they are given access to BARS. Accounts will be deleted by the BARS administrators when notified a user no longer needs access.

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 retained and disposed in accordance with the National Archives and Records Administration (NARA), Department Records Schedule 1- DAA-048-2013-0011 "Long-term Financial and Acquisition Records Reports". These records are temporary and will be destroyed by the agency 7 years after the system is decommissioned.

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

Equipment will be sanitized to remove all information from associated media prior to removal from the facility. Procedures from National Institute of Standards and Technology (NIST) 800-83 Guidelines for Media Sanitization will be followed based on the categorization of low for BARS.

DOI records are disposed of by 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.

BARS is a business management tool that performs budget and funding functions, and does not collect or maintain sensitive PII so there is minimal risk to the privacy of individuals throughout the information lifecycle. BARS analyzes financial data from FBMS for analysis and reporting purposes, and does not import PII from FBMS. BARS use of PII is limited to name and username for the purpose of managing and tracking user group assignments and user activities. All information is maintained within the system control of the agency. Data transmission is encrypted. All user and administrative actions are audited. To prevent misuse, the BOR system administrators review and analyze Active Directory audit records at least weekly. Only system administrators and the information system owner have access to system reports. There is no interconnection between BARS and FBMS Cloud. Only relevant data will be manually entered into the FBMS Cloud system. Any data added to BARS will come from a secure file transfer protocol site that does not connect to other systems.

The use of BARS is conducted in accordance with the appropriate DOI policy. BARS will undergo a formal assessment and authorization to attain an Authority To Operate (ATO) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and NIST standards before live production deployment. BARS is rated as FISMA “Low” based upon the type of data, and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the information contained in the system.

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); activities that could modify, bypass, or negate the system's security controls. All names recorded in the BARS audit logs and consolidated using audit monitoring tools are protected by only giving access to authorized personnel only. Backups of the audit logs can only be accessed by authorized users. Any equipment and media containing the audit logs that needs to be destroyed will follow the sanitization procedures outlined in NIST 800-83 Guidelines for Media Sanitization for low categorization systems.

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. BARS 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. All user activities captured by BARS in the audit logs are protected by giving access only to valid, authorized personnel. This information is not shared outside of BARS as this is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When BARS reaches end of life the equipment and/or media that contains user data and audit logs will be retained per the retention schedule for Information Technology systems and then destroyed.

There are mandatory requirements for employees and contractors of the DOI to complete training on information security, privacy, and records management before getting access to any DOI/BOR system. The Department emphasizes that Federal law and regulations require all Federal employees and other users of the Bureau of Reclamation information systems to receive this mandatory training and to acknowledge the Rules of Behavior, as presented in the course. To fulfill this requirement, all Reclamation employees, contractors, and other individuals who need access to Federal information systems and applications are required to complete all mandatory security, privacy, records management training during the onboarding process and on an annual basis.

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*

BARS generates audit records containing information that establishes:

1. what type of event occurred;
2. when the event occurred;
3. where the event occurred;
4. the source of the event;
5. the outcome of the event; and
6. the identity (user name) of any individuals or subjects associated with the event.

The DOI relies on its information technology systems, including the Budget and Reporting System (BARS), to accomplish its mission of providing cost-effective and reliable services to the DOI, other Federal agencies, and the public at large.

☐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?

BARS does not derive new data or create previously unavailable data about an individual through data aggregation.

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.*

Audit logs are consolidated via auditing tools for correlation, alerting, notification and reporting auditable events for devices within the SFC. Audit logs are primarily utilized for forensic and investigative purposes and used by the SOC personnel. Audit logs produced are configured to include type of event, the host that originated the log message, the date and time the event occurred, the application or command generating the event, the outcome of the event. Audit information is restricted to authorized-personnel only and designated in Active Directory security groups. These processes and procedures are outlined in the BARS System Security Plan.

☐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* BOR Information System Security Officer (ISSO) will have access to the system by request if there is a concern of a security incident. This type of access would be under the supervision of the System Owner or Project Manager.

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

BARS users will have access to financial data from FBMS Cloud, which does not include PII. Users will only have access to publicly available data in BARS which does not contain names of users. Users will not even have read access to any audit logs containing user names and associated events when they log in to BARS via DOI Active Directory. Only Systems Administrators will have access to BARS audit log data. By default, permissions on audit logs in Windows (operating system on which BARS resides) only allows access to administrators. In addition, the Manage auditing and security log user right for the logs is set only for Administrators also by default.

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?*

Contractors developed the system and contractors have hosting responsibilities to include the maintenance of BARS and the infrastructure and platform on which it resides.

A modification of the BARS contract is in progress to add the appropriate FAR Privacy Act Clauses and other privacy and security provisions in accordance with DOI policy.

☐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* BARS contains information system audit logs that identifies users and actions associated with their names.

☐No

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

User names can be associated with any of the following events and are captured in the BARS 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.

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

Access to BARS audit information and auditing tools are restricted to authorized-personnel only via access control lists. BARS information system audit logs are reviewed and analyzed at least weekly for indications of inappropriate or unusual activity and findings are reported to systems administrators and the ISSO. Security groups with access to audit logs are reviewed quarterly.

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* Visitors are escorted in 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. *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 Deputy Director of Program and Budget serves as the BARS Information System Owner and the official responsible for oversight and management of the BARS security and privacy controls. The Information System Owner is 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 BARS in collaboration with the BOR 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 BARS Information System Owner is responsible for oversight and management of the BARS security and privacy controls, and for ensuring to the greatest possible extent that BARS data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any suspected or confirmed compromise of data is reported to the DOI Computer Incident Response Center (DOI CIRC) and the proper DOI officials within 1-hour of discovery in accordance with Federal policy and established procedures.