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: Bureau of Reclamation Water Operations & Record Keeping System (BORWORKS)
Bureau/Office: Bureau of Reclamation/Denver
Date: August 26, 2021
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 Bureau of Reclamation Water Operations and Records Keeping System (BORWORKS) is a critical subsidiary accounting system that operates on the California-Great Basin Region's (CGBR) Local Area Network (LAN). It records the details of CGB's water accounting transactions and provides the following:

- Details of quantity and price of water transactions to achieve appropriate accountability fiscal integrity.
- Capability to record and generate reports of water delivery activity and revenue.
- Critical interface with Financial and Business Management System (FBMS) which is Reclamation's official financial system.
- Archival capability.

The data recorded and maintained in BORWORKS is used as follows: (1) the development and computation of water rates for Central Valley Project contractors and other non-project users; (2) preparation of water modeling scenarios; (3) water operations forecasts; and (4) water transfers. BORWORKS allows the CGBR to properly identify and account for water deliveries, payments, revenues, and provides data required in calculating annual water rates and determining cost recovery by water users. BORWORKS is a custom-designed software system that provides an automated means for updating and tracking water delivery, charge, and payment data for more than 250 long-term Central Valley Project water contractors, as well as hundreds of transactions for transfers, contracts, and water banking agreements within the CGBR. The CGB staff in the Regional Office (Accounting and Rate Setting) along with CGBR Area Offices record data in the system based on information received from respective water authorities or users. The information entered into BORWORKS is used to track water transactions, and subsequently used throughout the rate-setting process as a means of determining future water rates, deliveries and revenue, and ensuring the fair distribution of cost among water users.

BORWORKS uses Oracle software products and interfaces with FBMS which manages information for water customers for revenue and collection purposes. FBMS assigns customer identification numbers and provides confirmation on successful payment transactions.

C. What is the legal authority?

Reclamation Project Act of 1939 (43 U.S.C. Chapter 12); Project Operation Policy (P. L. 99-546) - A bill providing for the coordinated operation of the Central Valley Project and the State Water Project in California; Central Valley Project Improvement Act (P. L. 102-575); Section 2 of the Rivers and Harbors Act of 1937 (33 U.S.C. 7 Olg)

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

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

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

UII Code 010-000000278; BORWORKS System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
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)*

WBR-31, Acreage Limitation (64 FR 13234, March 17, 1999; modification published 73 FR 20949, April 17, 2008); WBR-40, Water Sales and Delivery Contracts (64 FR 29876, June 3, 1999; modification published 73 FR 20949, April 17, 2008); DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)"and DOI-86 FBMS-Accounts Receivable (73 FR 43772, July 28, 2008). DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ 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: *Specify the PII collected.* BORWORKS maintains the unique customer ID that is generated by FBMS to identify customers. Customer information is currently incorporated entities but legacy data does include names of individuals. Unique customer numbers generated by FBMS and names of individuals (legacy data) are maintained in BORWORKS. Usernames and passwords for employees who access the system are maintained in BORWORKS.

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

BORWORKS interfaces with FBMS which manages information for water customers for revenue and collection purposes. FBMS assigns customer identification numbers and provides confirmation on successful payment transactions.

☐ Other:

Paper Format – forms were used to collect information however the forms are no longer used and the forms are maintained as legacy data.

Employees complete an electronic access authorization form to request access to BORWORKS. Information collected includes employees name, work phone, work email address, supervisor's name, work phone, and work email address, as well as the requested access level for the system.

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

This information is used to identify revenue and collections data associated with water contracts.

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.*

Information is used by authorized Reclamation personnel to identify revenue and collections data associated with water contracts.

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

Information is used by authorized DOI personnel to identify revenue and collections data associated with water contracts.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Data may be shared with the Internal Revenue Service for the purpose of reporting the existence of "illegal Federal irrigation subsidies" as defined by Section 90 of the Internal Revenue Code and as outlined in the routine uses section of the published WBR-31, Acreage Limitation system of records notice.

Data may be shared pursuant to the routine uses contained in the published system of records notices DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and DOI-86, Accounts Receivable: FBMS.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Data may be shared to appropriate Federal, State, Tribal, or local agency that is responsible for investigation, prosecuting, enforcing, or implementing a statute, rule, regulation, order, or license when we become aware of an indication of a violation or potential violation of the statute, rule, regulation, order, or license as outlined in the published WBR-40, Water Sales and Delivery Contracts system of records notice.

Data may be shared pursuant to the routine uses contained in the published system of records notices DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and DOI-86, Accounts Receivable: FBMS.

☒ Contractor: *Describe the contractor and how the data will be used.*

Data may be shared with non-Federal auditors under contract with the Department of the Interior to perform audits relating to the acreage limitation program as outlined in the routine uses section of the published WBR-31, Acreage Limitation system of records notice.

☒ Other Third-Party Sources: *Describe the third-party source and how the data will be used.*

Data may be shared with financial institutions for the purpose of acquiring information needed by the lender to complete the certification and reporting requirements of the Reclamation Reform Act of 1982 for involuntarily acquired irrigable or irrigation land as outlined in the routine uses section of the published WBR-31, Acreage Limitation system of records notice.

Data may be shared with the State of California Water Resources Control Board for settlement of water rights if requested and only with proper DOI and/or Reclamation approval as authorized by the Privacy Act and outlined in the routine uses section of the published WBR-40, Water Sales and Delivery Contracts system of records notice.

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.*

Customers may decline to provide the requested information, however, if the information is not provided then the customer is not able to enter into a contract with Reclamation.

Reclamation employee information is voluntarily provided when requesting access to the DOI network and information systems, and normally occurs during the onboarding process and is required to enforce access controls across the DOI network. If users decline to provide the requested information, they will not be given access to the DOI network or BORWORKS.

☐ 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.*

Notice is provided through the publication of this PIA. Individuals may also view the WBR-31 "Acreage Limitation"; WBR-40 "Water Sales and Delivery Contracts"; DOI-86 "Accounts Receivable"; DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)" and DOI-86 FBMS- Accounts Receivable (73 FR 43772, July 28, 2008)system of records notices and related PIA for more information. DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

The following banner alerts users at the system's login screen:

***WARNING TO USERS OF THIS SYSTEM ***

This is a United States Government computer system, maintained by the Department of the Interior, to provide Official Unclassified U.S. Government information only. Use of this system by any authorized or unauthorized user constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. USERS HAVE NO REASONABLE EXPECTATION OF PRIVACY IN THE USE OF THIS SYSTEM. Unauthorized use may subject violators to criminal, civil and/or disciplinary action.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve

information (e.g., name, case number, etc.).

Data is retrieved by customer name and customer number.

I. Will reports be produced on individuals?

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

Reports are produced on and provided to individual water customers. These reports are used to provide water delivery information that include customer names (legacy data), entity name, customer identification numbers, acre feet of water delivered, payments, and charges. These reports are shared among authorized Reclamation and DOI staff.

☐ No

Section 3. Attributes of System Data

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

The data is collected from the individual water customer and it is the responsibility of the customer to provide accurate information.

B. How will data be checked for completeness?

The BORWORKS user obtains the data directly from the individual water customer and water contract. It is the responsibility of the individual water customer to provide complete data when entering into a contract with Reclamation.

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

Changes to the data are initiated by the individual water customer and documented via approval by the contracting officer in accordance with the terms of the applicable water contract.

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 permanent and are covered under the Reclamation records retention schedule WTR-4.03 “Water Sales/Delivery Contract/Exchange of Water” under the National Archives and Records Administration (NARA) approval authority N1-115-94-5, which is being incorporated into Departmental Records Schedule (DRS) 2.2.4.23

"Mission - Sustainably Manage Water - Historic Water and Power Projects, Resources and Delivery" currently pending approval by NARA. Until DRS-2 is approved BORWORKS records retention will be permanent. Once DRS-2 is approved BORWORKS records retention will remain permanent. Cutoff at end of fiscal year. Transfer to the FRC at 10 years or earlier if volume warrants. Transfer legal ownership to NARA 25 years after cutoff.

Records on user activity are retained in accordance with Departmental Records Schedule (DRS) – Administrative schedule 1.4 A.1 – [0013] Short Term IT Records – System Maintenance and Use Records (DAA-0048-2013-0001-0013). 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.

BORWORKS does not collect or maintain sensitive PII so there is minimal risk to the privacy of individuals. BORWORKS contains a minimal number of records of individuals names who have a water contract with Reclamation. There are risks that data may be inappropriately accessed or used for unauthorized purposes; users may not have adequate notice of the collection and use of their data; and that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. BORWORKS also contains records concerning corporations and other business entities, which are not subject to the Privacy Act.

Records in this system are permanent and are covered under the Reclamation records retention schedule WTR-4.03 "Water Sales/Delivery Contract/Exchange of Water" under the National Archives and Records Administration (NARA) approval authority N1-115-94-5, which is being incorporated into Departmental Records Schedule (DRS) 2.2.4.23 "Mission - Sustainably Manage Water - Historic Water and Power Projects, Resources and Delivery" currently pending approval by NARA. Until DRS-2 is approved BORWORKS records retention will be permanent. Once DRS-2 is approved BORWORKS records retention will remain permanent. Cutoff at end of fiscal year. Transfer to the FRC at 10 years or earlier if volume warrants. Transfer legal ownership to

NARA 25 years after cutoff.

The interface between BORWORKS and FBMS uses Secure File Transfer Protocol (SFTP), which is integrated with the Secure Shell (SSH) software package and provides data encryption between the systems. BORWORKS uses Transport Layer Security in conjunction with Secure Sockets Layer (SSL/TLS) for the web interface that users log into and it provides user session encryption. BORWORKS is necessary to track water revenue, collections and to comply with Federal laws and regulations. To control access and prevent misuse, employees must submit a formal account request and receive approval from organizational officials. The approved request is routed to the CGB Helpdesk for IT to grant the approved access role. BORWORKS administrators and Information System Security Officer (ISSO) establish and document user security roles and responsibilities. Continuous monitoring scripts automatically capture user audit logs which contain user login information, such as successful log-ins, failed log-ins, and account lockouts for the past 30 days. The user audit logs contain employee names, usernames, and date and time of attempted access.

The use of BORWORKS is conducted in accordance with DOI policy. BORWORKS undergoes recurring, formal Assessment and Authorization and has been granted an Ongoing Authority-to-Operate (ATO) in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. BORWORKS is rated as FISMA moderate based on the type of data and requires security controls to protect the confidentiality, integrity, and availability of the data contained in the system. BORWORKS application roles define specific access and permissions and individuals are granted access and permissions based on the role they are approved for. BORWORKS users must have a valid and authorized DOI Enterprise Active Directory account and their request for access to BORWORKS must be authorized and approved by the individual's Supervisor and the Finance office.

Separated employees are removed from the BORWORKS database by an authorized administrator upon receipt of an approved account termination from the separated employee's supervisor.

Users of DOI IT systems are expected to adhere to the DOI Rules of Behavior policy. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail includes 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 suspected attempts of unauthorized access or scanning of the system are investigated by IT Security personnel.

BORWORKS 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 security and privacy awareness and role-based training and sign DOI Rules of Behavior.

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

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 data is necessary for water delivery services and integration with FBMS.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☐ Contractors
☐ Developers
☒ System/Database Administrator
☐ Other: *Describe*

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

User access is limited as appropriate to the employees' position or role in the organization. User roles are approved by CGB Ratesetting Branch.

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 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*

Continuous monitoring scripts automatically capture user audit logs which contain user login information, such as successful log-ins, failed log-ins, and account lockouts for the past 30 days. The user audit logs contain employee names, usernames, and date and time of attempted access.

☐ No

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

All logins, failed logins, Oracle Fine-grained auditing, and database object changes.

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

BORWORKS is an internal-only application utilizing the Reclamation network and DOI Enterprise security perimeter to prevent unauthorized monitoring. The system monitoring is authorized and complies with the DOI Security Control Standards. Any attempts by individuals to monitor other individuals are covered by the DOI Rules of Behavior. BORWORKS user access is restricted through least privileges.

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 California-Great Basin Regional Director is the BORWORKS Information System Owner. The Information System Owner oversees and manages the protection of agency information processed and stored in BORWORKS. The BORWORKS Information System Owner and the Information System Security Officer (ISSO), in collaboration with the Privacy Act System Manager, California-Great Basin Region Privacy Officer and the Bureau of 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 BORWORKS.

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 BORWORKS Information System Owner is responsible for oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The BORWORKS System Owner and the 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 on individuals, in consultation with the California-Great Basin Region Privacy Officer and the Bureau of Reclamation Associate Privacy Officer.