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: Capital Asset and Resource Management Application (CARMA)
Bureau/Office: Bureau of Reclamation/Denver
Date: 4/13/2018
Point of Contact:
Name: Regina Magno
Title: Associate Privacy Officer
Email: privacy@usbr.gov
Phone: 303-445-3326
Address: PO Box 25007 (84-21000), Denver, Colorado, 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: *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 (BOR or Reclamation) uses the most cost-effective technology to support its asset and maintenance management program. The Capital Asset and Resource Management Application (CARMA) software system is based on a

commercial off-the-shelf software product called IBM ® Maximo® Asset Management software platform. CARMA, with Maximo™ as its base application, is Reclamation's computerized asset and maintenance management support system. The definition of effective and efficient asset management business practice standards, and the resultant configuration of CARMA, is important to the delivery of reliable, cost-effective services and products to Reclamation water and power customers.

The Bureau of Reclamation has four principal goals for the CARMA system:

- Delivery Reliability – Deliver as much water and power to customers as possible on a continuous and reliable basis.
- Cost Effectiveness – Deliver these products as inexpensively as possible while not compromising business principles and industry standards.
- Safety and Security – Maintain a high level of safety and security internally, as well as for the Public.

Information about individuals requiring access to CARMA is obtained from the Department of the Interior (DOI) Federal Personnel and Payroll System (FPPS) through an interface pathway to the Data Integration Data Distribution system (DIDD), which is a distribution hub that reads, partitions then distributes data to internal DOI applications such as CARMA, Electronic Time and Attendance System (ETAS), and the Financial and Business Management System (FBMS). Information about contract staff is provided to the CARMA Information System Security Officer by an authorized Manager or Supervisor at the facility following procedures outlined in the CARMA User Account and Password Management Standard Operating Procedure (SOP).

CARMA interfaces with the BOR Electronic Time and Attendance System (ETAS) to communicate labor hour transactions via CARMA work order numbers that are reported in ETAS by employees for payroll purposes.

C. What is the legal authority?

The Reclamation Act of 1902 and Reclamation Extension Act of 1914; Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulations); 5 U.S.C. 5514, 5701 et seq.; 26 U.S.C. 6402; 31 U.S.C. 3511 and 3512, 3701, 3702, 3711; 40 U.S.C. 483; Public Law 106-107, and 41 CFR 300-304.

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: 010-000000279 CARMA System Security Plan August 2016

☐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: DOI-85 - Payroll, Attendance, Retirement, and Leave Records

☐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: CARMA Person Identification number is auto-generated and associated with the CARMA user profiles, which allows BOR to authenticate users and manage permissions. Office location/address, work email address, work phone number, burden calculated pay rate, Supervisor's name and work phone number, labor identification number, and person identification number.

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:

DIDD sends data to CARMA from FPPS for the purpose of verifying the user is a Reclamation employee and auto-generating a CARMA PERSON ID, which is associated with the CARMA user profiles.

Reclamation is currently working on a single sign-on solution to require employees to access CARMA with government-issued Personal Identity Verification (PIV) card and personal identification number. The user's name and username data will be extracted from integration with the DOI Enterprise Active Directory (EAD) system, which authenticates users on the DOI network.

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

The PII is used to create a user profile in CARMA. 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.

After single sign-on is implemented, username data will be extracted from integration with the DOI EAD system, which authenticates users on the DOI 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.

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 the 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.*

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

CARMA users see a login banner when entering the system. Users are required to 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 CARMA. Individuals have the option of declining to access the CARMA application, however, their pay may be impacted since their time and attendance will not be completed for the related work orders.

☐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 also provided through the publication of this PIA and the system of records notice: DOI-85 - Payroll, Attendance, Retirement, and Leave Records

☒Other: *Describe each applicable format.*

To logon to a BOR computer, a DOI Warning Banner appears which states the user understands all activity is tracked and not private.

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.).

Data can be retrieved by searching username, first and last name, labor identification number, and person identification number, which is a unique identifier for users in the CARMA system.

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.

Quarterly user reports are generated in CARMA which identify the username, last login, number of login attempts, and date of login. These reports are stored in CSAM as part of security control protocols. Only authorized users of BOR CSAM can access these reports in CSAM. Labor and person-related records will be available in CARMA that identify the person's name, username, crew work availability, location, and the individual's specialized craft for work assignment.

Managers, supervisors, planners and maintenance craft personnel will utilize the labor identification number and person identification number to create labor reports and cost associated reports. The Business Owner, System Administrator, CARMA Project Manager, Information System Security Officer (ISSO), and others with privileged level access to CARMA may request and be granted access to audit logs on a need to know basis.

☐No

Section 3. Attributes of System Data

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

CARMA does not collect data from sources outside of the DOI. The user will enter their "user name" and password to access the application. BOR employees enter their own time and attendance, and other information related to work orders.

B. How will data be checked for completeness?

BOR employees enter their own time and attendance, and other information related to work orders, which are expected to be complete for each pay period. The CARMA system authenticates the username and password when the user logs into CARMA.

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

Employees enter their own time and attendance, and other information related to work orders, which is current for each pay period. Employee data (Name, email address, work phone and address) are verified when CARMA user profiles are established.

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

Records for the system are covered by Department Record Schedule (DRS) Code 2.2.4.21 "Mission – Sustainably Manage Water – Non-Historic Water and Power Projects and Facilities" which has been approved by the National Archives and Records Administration (NARA)(N1-115-94-8). Temporary (Long-Term). Cutoff when facility or structure ceases to exist, is transferred to a non-DOI entity, records are no longer needed for continued operation of the structure or feature, or at the completion of project activities. Destroy 10 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). These records have a temporary disposition. Records are cut-off when obsolete and destroyed no later than 3 years after cut-off.

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

Approved disposition methods include 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.

CARMA is Reclamation's computerized asset and maintenance management support system that collects and maintains non-sensitive PII such as name, labor hours, and official contact information so there is minimal risk to the privacy of individuals throughout the information lifecycle. CARMA interfaces with BOR's ETAS system to communicate labor hour transactions via CARMA work order numbers that are reported in ETAS by employees for payroll purposes. CARMA's 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 administrator's review and analyze audit records at least monthly. Only system administrators and the information system owner have access to system reports.

The use of CARMA is conducted in accordance with the appropriate DOI policy. CARMA has undergone 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 National Institute of Standards and Technology (NIST) standards. CARMA is rated as FISMA "Moderate" 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 CARMA 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. CARMA 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 CARMA in the audit logs are protected by giving access only to valid, authorized personnel. This information is not shared outside of CARMA as this is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When CARM 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 DOI employees and contractors to complete training on information security, privacy, and records management before acquiring access to any DOI and BOR system. DOI emphasizes that Federal law and regulations require all Federal employees and other users of BOR 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.

The CARMA ISSO works closely with the facility Managers, Supervisors and CARMA users to ensure only current and authorized users have access to CARMA and that data about individuals is complete and accurate. Monthly employee separation reports are provided to the CARMA ISSO in order to deactivate CARMA user accounts of employees who are no longer employed with BOR.

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*

The data is relevant and necessary in order for individuals to access CARMA and document labor and work performed on BOR assets.

☐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. CARMA does not derive new data on individuals.

F. Are the data or the processes being consolidated?

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

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

☒No, data or processes are not being consolidated.

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

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

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

Access to the system is granted through the assignment of one or more roles, the privilege to read or modify data that is required to perform the duties of their jobs. Managers and supervisors are responsible to ensure that the privileges granted are necessary. Also, the CARMA User Account and Password Management Standard Operating Procedures provides information on how user access is determined.

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?*

The IBM contract for IBM Maximo Asset Management software licenses is managed by DOI. The services and support contract is managed by BOR. Both contracts include Privacy Act contract clauses.

☐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*
The CARMA user reports collect information on users such as login id, last login date, last login time, status of user account, and user location.

☐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 CARMA 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?

The CARMA ISSO has overall responsibility for controlling user access and ensuring accomplishment of user access management reviews, including working closely with the CARMA administrator to ensure that proper managerial and technical controls of security within CARMA are followed.

The CARMA administrator is responsible for the software configurations, including security, and will work closely with the CARMA ISSO to ensure the proper managerial and technical controls of security within CARMA are followed. Also, the CARMA administrator is responsible for ensuring "User Security Groups" are created in Maximo, and group privileges are properly set for the Groups. Security configuration management in Maximo will be managed through the CARMA Change Management Standard Operating Procedures.

Within Maximo, users are given privileges by the CARMA ISSO to access and use features of the software. Security needs of CARMA necessitate the central management of user accounts and this will be done by the CARMA ISSO in Denver. Users of CARMA also have responsibilities for maintaining security precautions.

Access logs will be monitored and reviewed by the CARMA ISSO quarterly via four user reports within CARMA. These are the report names: Login Tracking Report, User Inactivity Report, User List by Status and Site Report, and Users not logged in Report. Any inappropriate activity will be reported according to the incident management policy to the CARMA project manager. The CARMA ISSO generates these user reports as mandated by the NIST security controls for CARMA.

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 Director, Policy and Administration, is the CARMA Information System Owner. The System Owner oversees and manages the protection of agency information processed and stored on CARMA. The CARMA System Owner and ISSO, in collaboration with 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 CARMA.

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 CARMA 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 CARMA 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 on individuals, in consultation with the Reclamation Associate Privacy Officer.