

U.S. Department of the Interior
Bureau of Reclamation

**Capital Asset and Resource Management
Application (CARMA)**

Project Number: [010-10-01-07-00-003]

Privacy Impact Assessment

February 2010



Prepared for the Department of the Interior

1849 C Street, NW, Washington, DC 20240

**Department of the Interior
Bureau of Reclamation
Privacy Impact Assessment**

Name of Project: Capital Asset and Resource Management Application (CARMA)

Bureau: Bureau of Reclamation

Office: Maintenance Services Division (84-57000)

Project's Unique ID:

The Department of the Interior (DOI) has overall responsibility for systems that are based on the software Maximo™ and its system is called Facility Management System (FMS). The DOI System Identification number for FMS is 010-010-01-07-00-003. CARMA is a step toward Departmental consolidation of all Maximo™ systems under Reclamation's umbrella of FMS. Therefore, CARMA does not have a Project Unique ID.

A. CONTACT INFORMATION:

- 1) Who is the Bureau/Office Privacy Act Officer who reviewed this document?**
Casey Snyder, Privacy Act Officer
Information Management Division, 84-21300
Denver, Colorado
303-445-6575

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any information about individuals?**
Yes
 - a. Is this information identifiable to the individual¹? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).**
No

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- b. Is the information about individual members of the public? (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).**

No

- c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).**

Yes

- 2) What is the purpose of the system/application?**

Asset and Maintenance Management support for Reclamation facilities.

- 3) What legal authority authorizes the purchase or development of this system/application?**

The Reclamation Act of 1902, as well as Human Resources and Payroll Systems Requirements (GAO AIMD-00-21.2.3). This requirements document can be found at: <http://www.gao.gov/special.pubs/ai002123.pdf>.

C. DATA in the SYSTEM:

- 1) What categories of individuals are covered in the system?**

Individuals covered in the system are Reclamation employees and contractors.

- 2) What are the sources of the information in the system?**

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Information about the individual comes from the Federal Personnel and Payroll System (FPPS) through an interface to the Corporate Data Warehouse (CDW). Information about contract staff is provided to the CARMA SSM by an authorized Manager or Supervisor at the facility following procedures outlined in the CARMA User Account and Password Management Standard Operating Procedure (SOP).

- b. What Federal agencies are providing data for use in the system?**

National Business Center (NBC), FPPS and the Federal Financial System (FFS) Central Contractor Registration (CCR) through the NBC Reclamation

c. What Tribal, State and local agencies are providing data for use in the system?

Not Applicable

d. From what other third party sources will data be collected?

Not Applicable

e. What information will be collected from the employee and the public?

No information will be collected from employees or the public. Information about employees comes from the source system FPPS.

3) Accuracy, Timeliness, and Reliability

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

Managers or Supervisors at a facility are responsible for requesting and reviewing the access of contract employees based on information provided to them from the Contracting Officer's Representative overseeing the contract. CARMA will not contain a contractor's social security number or any other personally identifiable information.

b. How will data be checked for completeness?

The CARMA System Security Manager 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.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes. CDW downloads employee data from FPPS, financial data from FFS, and vendor data from the NBC on a daily basis and distributes to CARMA via interfaces. Database Administrators (DBAs), monitor the interfaces and take appropriate action if a failure is detected.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. Employee data elements are described in the FPPS metadata maintained by the NBC. There is a data model of CDW that supports how the employee, financial and vendor data is housed in CDW. Data elements unique to Maximo™, the base software of CARMA, are described in a data model from the vendor of Maximo™, as well as in the Oracle database that supports Maximo™. Technical documentation also exists that describes how Maximo™ data elements were configured to support unique requirements of Reclamation.

D. ATTRIBUTES OF THE DATA:

- 1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No.

- 3) **Will the new data be placed in the individual's record?**

Not Applicable.

- 4) **Can the system make determinations about employees/public that would not be possible without the new data?**

Not Applicable.

- 5) **How will the new data be verified for relevance and accuracy?**

Not Applicable.

- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

All access to data by end users will be done through Maximo™ user accounts that are assigned one or more groups, and are given privileges to access one or more sites. A Maximo™ group is given specific read, write, insert, or delete privileges. NO end user will access the Maximo™ database with any tool or application besides Maximo™. The CARMA User Account and Password SOP define the controls for protecting data for unauthorized access or use.

Maximo™ contains the feature known as “SITE”. A SITE is a software based segregation of data to prevent all data being seen by all users. For example, CARMA has unique SITES for Hoover, Folsom, Grand Coulee, and Glen Canyon, and only through explicit authorization from those sites will end users be able to see data.

End users must read and sign the Reclamation General Rules of Behavior document which gives guidance of their responsibility for protecting data.

DBAs can access all of the CARMA data; however, through the separation of duties of the DBAs, no one DBA will have access to all environments; i.e., development, testing and production. A policy is in place in all Oracle databases that monitors the username, login, and logout times to further provide control and information on access.

System Administrators (SAs) do not have access to the backend Oracle databases. SAs, however, will be given a unique Maximo™ account, group, and privileges to be used exclusively to verify that Maximo™ is operational when they are providing technical support.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

CARMA, more specifically, Maximo™ user accounts will be centrally managed in the Denver Office by the CARMA System Security Manager in collaboration and cooperation with the CARMA Administrator. The roles and responsibilities of these administrators are described in the CARMA User Account and Password Management Standard Operating Procedure. In addition, the following administrators will also administer and control different aspects of CARMA, more specifically, access to Maximo™ data:

- Property Administrator – Responsible for creating item masters and storerooms.
- Report Administrator – Publishing reports and granting privileges to execute reports to end users.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

CDW provides the Integration Server calculated burdened rate for every Reclamation employee by social security number.

Information about a person is retrieved by a random-generated, unique identifier (ID). This ID then retrieves the person's full name and displays the ID and name on the screen for the end user. Also, an end user can query on a person's name or ID.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Labor and person-related records will be available in Maximo™ that will describe the person's name, ID, availability to do work, location, and relationship to work they have been assigned to do. These reports contain no information covered by the Privacy Act.

Managers, supervisors, planners and maintenance craft personnel will utilize the labor and person-related records most often; however, the Business Owner, System Manager, System Security Manager, Property Administrator, and other with login accounts to Maximo™ may request and be granted access to these reports.

From ETAS: labor transaction information.

From CARMA: labor codes, person ID, work order information.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

None. Individuals who work at a Reclamation facility and can potentially perform work at the facility will have information about them stored in the database.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Maximo™ stores information about a person at the organization level. An organization level is a logical separation of the data that allows all sites (another separation of data) to have access. Sites, on the other hand, are a logical separation of data that allows only privileged individuals at the particular site to see the data.

Information about a person is not entered by a CARMA end-user but rather through an automated interface using FPPS source data and information supplied to the CARMA Security Manager by managers or supervisors overseeing contract staff.

2) What are the retention periods of data in this system?

At this time, no discussions have taken place to indicate that data will not be kept indefinitely. The system belongs to DOI and therefore they are responsible for submittal of the BC 300 and records retention requirements to NARA/OMB for approval.

- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
Because of lack of clarity on retention periods as it related to asset and maintenance management data, this question is not being answered.
- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No.
- 5) **How does the use of this technology affect public/employee privacy?**
Not applicable.
- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
See response to question E9 of this document.
- 7) **What kinds of information are collected as a function of the monitoring of individuals?**
See responses to questions E8 and E9 of this document.
- 8) **What controls will be used to prevent unauthorized monitoring?**
It is the responsibility of managers and supervisors at the facilities to prevent unauthorized monitoring of individuals.
- 9) **Under which Privacy Act Systems of Records Notice does the system operate? Provide number and name.**
CARMA will operate under the FPPS Systems of Records Notice.
- 10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
Not applicable.

F. ACCESS TO DATA:

- 1) **Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

Reclamation employees and contractors working for Reclamation will have access to data.

- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Reference the CARMA User Account and Password Management SOP for information in how user access is determined.

- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Anyone who has access to the system will be 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, reference the CARMA User Account and Password Management SOP for information in how user access is determined.

- 4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**
Managers

The CARMA Security Manager has overall responsibility for controlling user's 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. Specifically, the CARMA Security Manager is responsible for the following:

1. Use the Maximo software to manage user accounts and passwords. The CARMA Security Manager is trained in the use of the application and the procedures to be followed. The CARMA Security Manager will work closely with the Site Managers, Supervisors, and CARMA users to ensure only current and authorized users have access to CARMA.
2. Authorize the RESC to create HEAT tickets for all user account requests (create, modify, suspend, or delete), and resetting of user account passwords.

3. Take action to remove user accounts of separated Reclamation employees within the same month as receipt of the Separated Employees List from the Denver Office IT Security Manager.

The CARMA Administrator is responsible for the software configurations, including security, and will work closely with the CARMA Security Manager 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 Change Management Standard Operating Procedures.

The CARMA software system is based on a commercial off-the-shelf software product called “Maximo Enterprise Suite (MXES)”. Within MXES users are given privileges by the CARMA Security Manager 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 Security Manager in Denver. Users of CARMA also have responsibilities for maintaining security precautions. Access logs will be monitored and reviewed by the CARMA SSM monthly via a report from Maximo. This report is under development. Any inappropriate activity will be reported according to the incident management policy to the CARMA project manager. The CARMA Administrator and the CARMA System Security are formulating a plan for auditing which would address user activities.

The Installation ITSM and the Reclamation BITSM are responsible for assisting the CARMA Team in the proper handling procedures of incidents.

RMSS and RecNet have monitoring processes in place to detect inappropriate activities. See the RMSS and RecNET system security policies and other documentation for more information.

- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes.

- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**

Yes. CARMA interfaces to ETAS and to CDW.

Employee data from FPPS distributed to CARMA. This contains Privacy Data. This is done within the Maximo Enterprise Adapter.

Organization codes from FFS are distributed to CARMA. This is done within the Maximo Enterprise Adapter.

Account structures from FFS distributed to CARMA. This is done with Oracle replication technology. Please see ORA-SOP-061 for more information.

All work orders that have a status that are a synonym of approved or completed. CARMA sends this data to ETAS via the Integration Server. There is no privacy data in this transmission.

Labor transactions (person, TAAS ID (social security number), pay code, hours charged, date charged). ETAS sends this data to CARMA via the Integration Server and the Maximo Enterprise Adapter. The TAAS ID is privacy data. CDW provides the Integration Server calculated burdened rate for every Reclamation employee by social security number.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
The Corporate Information Services Group and the CARMA Security and System Managers, all based in Denver, have the overall responsibility of ensuring the privacy rights of employees affected by interfaces.
- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**
No.
- 9) How will the data be used by the other agency?**
Not Applicable.
- 10) Who is responsible for assuring proper use of the data?**
The Maintenance Services Division, as well as manager and supervisors at Reclamation facilities.