April 1, 2013

Department of the Interior
Privacy Impact Assessment

Name of Project: Corporate Data Warehouse
Bureau: Bureau of Reclamation
Project's Unique ID: 010-10-01-01-01-1010-00-403-132

A. CONTACT INFORMATION:

Regina Magno-Judd
Privacy Act Officer
Information Management Division, 84-21300
303-445-2056
rmagnojudd@usbr.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes – Includes name, social security number (SSN), base salary, **individual's bank and bank account number**, individual's leave information, and a consolidation of Technical Service Center employee's time and attendance charges to financial account structures.

The Corporate Data Warehouse (CDW) major application provides Bureau of Reclamation (Reclamation) user communities with access to timely, reliable information by creating and provisioning a consolidated financial, human resource, and performance goals and metrics data repository. This eliminates the need for creating and maintaining data and reports from separate transaction systems. Data types include employee data, financial data, organization codes and other information used for payroll processing. The CDW is a warehouse that stores PII from the following six systems:

- The Interior Department Electronic Acquisition System (IDEAS)-Procurement Desktop (PD) major application, part of the Department of the Interior's (DOI) IDEAS-PD, may contain information about individuals within government vendor data. IDEAS-PD contains large, small, and sole proprietorship business information that identifies the name of the company and the company's Tax Identification Number issued by the Internal Revenue Service. Some small businesses choose to use their personal names as their business name and their SSN as their Tax Identification Number. Reclamation has no control over such use. Although IDEAS-PD is a Departmental system, Reclamation's subsystem component is supported by the Reclamation Mission Support System

(RMSS) and is considered a major application; its PII is described in a separate PIA, the *IDEAS-PD Privacy Impact Assessment.*

- The Electronic Time and Attendance System (ETAS) major application is a Reclamation-wide application that provides a common means for Reclamation employees and management to enter, validate, and approve time and attendance data. The system contains employee personal information including names and corresponding SSNs. Although efforts are made to maintain segregation between names and SSNs, both types of information do reside within the system. Since ETAS is considered a major application, its PII is described in a separate PIA, the *ETAS Privacy Impact Assessment.*

- The Capital Assessment and Resource Management Application (CARMA) is a Reclamation-wide major application that is identified as a sub-component of the DOI Enterprise-wide Asset Management (Maximo) system. It provides a common means for DOI (Reclamation) staff to manage capital and human resource assets. The system contains employee personal information derived from the DOI Federal Personnel and Payroll System (FPPS).

- Technical Service Center Management Information System (TSCMIS). The Bureau of Reclamation Technical Service Center (TSC) new Management Information System (TSCMIS) is an IT portfolio investment that provides automated support to TSC engineering organization business processes and activities related to reimbursable engineering and analytical services for managing, protecting, and developing water and related resources. TSCMIS facilitates Reclamation's TSC workflow and project management process by providing a data entry and management system to: input staff day estimates, schedules and scope of work for Service Agreements (SA) with clients, capture and maintain Task-Based Estimates (TBE) and for resource management, calculate budgets based on the estimated staff days and non-labor input, enter and maintain the TSC billable rate structure and create contract SA specific billing information for TSC work (i.e., the billable rate file)

  TSCMIS supports the work of approximately 560 engineers, scientists and support personnel who provide specialized technical engineering and analytical services to a wide variety of clients in BOR and other government agencies on an optional-use fee-for-services basis. TSCMIS allows for and maintains contract specific activity

- Electronic Service Agreement Module (ESAM) is a Bureau of Reclamation (Reclamation) IT portfolio investment that encompasses two IT systems for the FY 2011 transition period: (1) The current system, Technical Service Center Management Information System (TSCMIS) used exclusively by the Technical Service Center to manage technical service agreements; and (2) its replacement, the Electronic Service Agreement Module (ESAM). ESAM is a refreshed version of the service agreement module in TSCMIS that will be deployed to nine technical service sites Reclamation-wide in FY 2012. TSCMIS will be decommissioned once Technical Service Center users are migrated to ESAM.

These systems support the work of approximately 1,400 engineers, scientists, and support personnel, and provide automated support to engineering organization business processes and activities related to reimbursable engineering and analytical services for managing, protecting, and developing water and related resources. The systems facilitate workflow and project management processes by providing a data entry and management system to:

- Input staff day or line-item task estimates
- Input schedules
- Input scopes of work for Service Agreements (SA) with clients
- Calculate budgets based on the estimated staff days and non-labor input
- Track job status and cost effectiveness of the services provided
- Support workload distribution
- Enter and maintain billable rate structures
- Create contract SA specific billing information

In some of the installations, these systems interface with Reclamation's Electronic Time and Attendance Automated System (E-TAS) and Federal Finance System (FFS) to collate individual charges by employees, organize those charges in a manner which allows accurately tracking of those charges against client accounts, and bill those accounts based on the appropriate billable rate cost structure.

Utilization of ESAM by all Reclamation Technical Service Providers (TSP) will increase the transparency and accountability of cost associated with in-house technical services and will support organization-wide work load planning and distribution initiatives. Reclamation's Coordination and Oversight Group will oversee and recommend improvements to agency workload planning based in part on data available via ESAM. These activities are to address some of the recommendations noted in the 2006 National Research Council Report, "Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation" concerning Reclamation's organizational structure and maintenance of technical capabilities.

- Reclamation Mission Support system (RMSS) is a set of Information Technology (IT) resources within and across Reclamation and its regional, area, project, and field offices that supports mission-related business operations, responding as needed to changing requirements and improved technology.

  A general review of the data elements in the system was performed and no public personal information was found. However, due to the vast amount of components in the RMSS, a more thorough inventory will be done to ensure initial findings are correct.

  All information security controls, other than those associated with RMSS, are the responsibility of the major applications identified as part of Reclamation's IT portfolio. Therefore, while RMSS components may access or transport identifiable information about individuals, RMSS is not responsible for not is it identified in this assessment as a system with privacy impact since all encryption or other application layer security measures necessary to protect the privacy of individuals must be provided by the applicator.

a. Is this information identifiable to the individual[1]?

Yes, by name and SSN.

- RMSS GSS – N/A. Refer to the *RMSS Privacy Impact Assessment*
- ETAS Major Application – Yes. Refer to the *ETAS Privacy Impact Assessment*
- IDEAS-PD Major Application – Yes. Refer to the *IDEAS-PD Privacy Impact Assessment.* Although not required by law, some businesses choose to use their personal names as their company name and their SSN as their company's Tax Identification Number.
- CARMA Major Application – Yes. Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – No. Refer to the TSCMIS *Privacy Impact Assessment.* A review of the data elements in the system was performed and there is no personal information in the system.
- ESAM Major Application – No. Refer to the ESAM *Privacy Impact Assessment.* A review of the data elements in the system was performed and there is no personal information in the system.

b. Is the information about individual members of the public?

- RMSS GSS – N/A

- ETAS Major Application – No. Refer to the *ETAS Privacy Impact Assessment*

- IDEAS-PD Major Application – Yes. See B.1) a., bullet 4, above.

- CARMA Major Application – No. Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – No. Refer to the TSCMIS Privacy Impact Assessment. A review of the data elements in the system was performed and there is no personal information in the system.

- ESAM Major Application – No. Refer to the ESAM Privacy Impact Assessment. A review of the data elements in the system was performed and there is no personal information in the system.

c. Is the information about employees?

- RMSS GSS – N/A

- ETAS Major Application – Yes. Refer to the *ETAS Privacy Impact Assessment*

- IDEAS-PD Minor Application – No

- CARMA Major Application – Yes. Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – No. Refer to the TSCMIS *Privacy Impact Assessment.* A review of the data elements in the system was performed and there is no personal information in the system.

[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).

- ESAM Major Application – No. Refer to the ESAM *Privacy Impact Assessment.* A review of the data elements in the system was performed and there is no personal information in the system.

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

The CDW is a centralized Oracle data warehouse which provides different user communities and user types with access to timely, reliable information by creating and provisioning a consolidated financial, human resource, and performance goals and metrics data repository; thus eliminating the need for creating and maintaining reports from the transaction systems. The CDW has two main features:

- **Reporting:** The 1994 implementation employed an industry standard reporting tool (i.e., Cognos Corporation's Impromptu tool) that enabled the creation and easy maintenance of standard look and feel enterprise-wide management reports. This system enables the creation and easy maintenance of standard look and feel enterprise-wide management reports (a.k.a. FIRS) as well as provides a single solution for acquiring and distributing operational data (personnel, financial) to Reclamation applications. Finally, the system provides for a single source for standard financial, human resources, and performance management historical data for managers across Reclamation.

  Data applicable to the Privacy Act exists in the following subject areas in the CDW:

  - Labor Cost
  - Employee
  - BOR Financial
  - Job Corps Financial
  - Billable Rates

- **Data Services:** Reclamation Financial and Employee Data is made available to other systems such as E-TAS, TSCMIS, ESAM, and CARMA. Data types include employee data, financial data, organization codes and other information used for payroll processing.

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

The CDW project had its genesis in a Reclamation-wide study of perceived management financial reporting inadequacies. The Financial Information Reporting Team conducted the study and reported its results in June 1993. At the direction of the Reclamation Chief Financial Officer and his CFO Steering

Committee, the team developed the initial warehouse, titled Financial Information Reporting System (FIRS) in October 1993 and deployed it Reclamation-wide in July 1994. This system was subsequently converted from the Ingres database to the Oracle database in 1996, and updated to comply with a Corporate Data Architecture strategy.

C. DATA in the SYSTEM:

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

Federal and contract employees.

- RMSS GSS – N/A
- CDW Major Application – Employees
- ETAS Major Application – Employees
- IDEAS-PD Major Application – Vendors doing business with the Government
- CARMA Major Application – Employees
- TSCMIS Major Application – Employees but not specifically.
- ESAM Major Application – Employees but not specifically.

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?

FFS (Federal Financial System)
BOR Labor Cost System
FPPS (Federal Personnel and Payroll System)
NewMIS/TSCMIS (New Management Information System / Technical Service Center New Management Information System)
Directly from individuals

- RMSS GSS – From the businesses themselves.
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS-PD Major Application – The source of any individual information in IDEAS-PD is the vendors themselves. Some confirmation can be accomplished by comparing the submitted information to GSA's Central Contracting Registry (CCR). Vendors who wish to do business with the Federal Government are required to register in CCR. Vendors can voluntarily submit their information to individual agency components employing IDEAS-PD.

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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

National Business Center, Denver, CO
Reclamation

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the TSCMIS Privacy Impact Assessment

- ESAM Major Application – Refer to the ESAM Privacy Impact Assessment

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

- RMSS GSS – N/A

- ETAS Major Application – None. Refer to the *ETAS Privacy Impact Assessment*
- IDEAS-PD Major Application – None. Refer to the *IDEAS-PD Privacy Impact Assessment*
- CARMA Major Application – None. Refe*r to the CARMA Privacy Impact Assessment*
- TSCMIS Major Application – None. Refer to the *TSCMIS Privacy Impact Assessment*
- ESAM Major Application – None. Refer to the *ESAM Privacy Impact Assessment*

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

None.

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

None from the public
Employee
Full legal name
Technical Service Center only – daily time and attendance records (hours marked pay code, financial account number charged)

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*
- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

3) Accuracy, Timeliness, and Reliability

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

All records are from DOI sources or from individuals. Accuracy is verified in the following ways during the loading process:

1. The number of records are counted in the source file and then compared against the number of records loaded into the Oracle tables to ensure all records are loaded successfully.
2. Log files generated during the loading process are reviewed to determine if any errors were encountered and if so, the errors are corrected and the data is reloaded.
3. Data stewards for billable rates, financial and labor cost data review the data daily for accuracy.
4. The employee data file is created by FPPS for Reclamation use and is verified as correct by FPPS. During the download of this data, record counts are taken and logs of the loading process are reviewed for accuracy. Also, employee data is verified by Reclamation Timekeepers as they use the data in the Electronic Time and Attendance System (E-TAS).
5. Information collected from individuals is verified by local Coordinators that assist in the management of user accounts.

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

b. How will data be checked for completeness?

Data stewards review the data on a daily basis to determine the completeness and accuracy of the loads to the CDW.

The number of records are counted in the source file and then compared against the number of records loaded into the Oracle tables to ensure all records are loaded successfully.

Log files generated during the loading process are reviewed to determine if any errors were encountered and if so, the errors are corrected and the data is reloaded.

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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).

Data applicable to the Privacy Act are updated either daily, bi-weekly, monthly, or at the end of the fiscal year from the source systems. Specifically, the schedules for updates are:

Labor Cost – Biweekly
Employee – Daily
Billable Rates – Biweekly
Financial – Daily, Monthly, End of Fiscal Year

A data model, which is under change management, is maintained to describe the CDW Oracle database environment. File descriptions are maintained to describe the source system environments. Any changes to the CDW environment are managed through a formal Change Request process.

Data collected from individuals are verified as current by local Coordinators who keep the CDW Project Manager informed of any necessary adjustments in the data.

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*
- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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

The source systems for the subject areas in CDW maintain metadata on the data elements. The CDW data model describes in more detail the data elements as they exist in the Oracle database.

- RMSS GSS – Yes. Refer to the *Information System Security Plan* and the *FIPS 199 Categorization Form* for RMSS.
- ETA*S Major Application* – Yes. Refer to the *Information System Security Plan* and the *FIPS 199 Categorization Form* for ETAS.
- IDE*AS PD Major Application* – Yes. Refer to the *Information System Security Plan* and the *FIPS 199 Categorization Form* for IDEAS PD.
- *CARMA Major Application* – Yes. Refer to the *Information System Security Plan* and the *FIPS 199 Categorization Form* for CARMA.

- TSCMIS Major Application – Yes. Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Yes. Refer to the *ESAM Privacy Impact Assessment*

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?

- RMSS GSS – N/A. RMSS is a general support system and provides computing resources and network services for other systems and applications. Refer to the documentation for individual systems/applications hosted by RMSS for details regarding the relevancy of data.

- CDW Major Application – Yes. Refer to the CDW I*nformation System Security Plan*.

- ETAS Maj*or Application – Yes. Refer t*o th*e ETAS Privacy Impact Assessment* and *Information System Security Plan*.

  IDEAS-PD Major Application – Yes, the use of the data is both relevant and necessary for the purpose of IDEAS-PD. The awards of Federal contracts are only authorized by the Central contracting Registry (CCR) registered vendors. If the vendor is not registered in CCR, IDEAS-PD will not allow an award to be processed. Refer to the *IDEAS -PD Privacy Impact Assessment* and *Information System Security Plan*.

- CARMA Major Application – Yes. Refer to the *CARMA Privacy Impact Assessment* and *Information System Security Plan*.

- TSCMIS Major Application – Yes. Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Yes. Refer to the *ESAM Privacy Impact Assessment*

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?

Yes. All data about an individual is available in the source systems. However, through the aggregation of data during reporting from the CDW new information about an individual is created. For example, there are individual records from FPPS that contain an employee's name and individual records from Labor Cost that contain information on how much an employee charges to a certain fund that when joined together during reporting creates a record that shows an employee's name and charges together.

New derived data is created on-demand during reporting and is not permanently maintained or filed.

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS-PD Major Application – No, IDEAS-PD is neither designed to collect individual information nor to aggregate this information.
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – No. Refer to the TSCMIS Privacy Impact Assessment
- ESAM Major Application – No. Refer to the *ESAM Privacy Impact Assessment*

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

No. New data is derived through reporting only and no permanent copy of the "new" derived data will be retained in CDW.

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS-PD Major Application – N/A
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – No. Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – No. Refer to the *ESAM Privacy Impact Assessment*

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

Yes. For example, through reporting, a manager can analyze employee availability and costs to perform work activities at specific points in time by examining employee leave balances, salaries, and work schedules.

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS-PD Major Application – No, IDEAS-PD is not used to make determinations about employees. IDEAS-PD validates vendor submitted data against the CCR to ensure the eligibility of a vendor to do business with the Federal Government.

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – No. Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – No. Refer to the *ESAM Privacy Impact Assessment*

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

Data stewards, who at this time are also the Corporate Impromptu report writers, verify the relevance and accuracy of the new derived data as it relates to standard corporate reports. New data derived by individual users during ad-hoc queries or report generations are verified as correct only by the individual.

- RMSS GSS – N/A

- ETAS Major Application – Refer to th*e ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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

The CDW consists of two centralized databases which are comprised of multiple Oracle schemas which service different operating aspects of the CDW. Each schema has slightly different controls in place to protect the data and the controls are based on the category of user accounts. Procedures for creating and maintaining database administrator accounts (which each schema has) are documented in the *Oracle Security SOP, ORA-SOP-011*. These accounts are password protected and only those privileges necessary to perform the specific activities are granted to the accounts. The following describes the controls for each schema.

CDWADM Schema

This schema supports the CDW Security Application which provides IT staff the capability to manage general user accounts and gives general users the capability to change their own passwords. General user accounts are under password change control and meet the requirements established in the Directive and Standard IRM 08-12, Computer Protections, Anti-Virus, Access Control and Passwords. There is a procedure in place, established December 29, 2003, that controls the establishment, maintenance and removal of general user accounts and changes to accounts are authorized by local, regional Coordinators who know the users. Further, general user accounts have an Oracle role assigned to them that gives only those privileges necessary to read the data thereby further protecting the data from being altered.

DWADM Schema

This schema is the main structure for general users to access and run reports. General user accounts are under password change control and meet the requirements established in the Directive and Standard IRM 08-12, Computer Protections, Anti-Virus, Access Control and Passwords. There is a procedure in place, established December 29, 2003, that controls the establishment, maintenance and removal of general user accounts and changes to accounts are authorized by local, regional Coordinators who know the users. Further, general user accounts have an Oracle role assigned to them that gives only those privileges necessary to read the data thereby further protecting the data from being altered. Finally, all general users of the CDW are required to sign a CDW Rules of Behavior document which further outlines what a user cannot do with their accounts.

REPADMIN Schema

This schema is used to manage the Oracle replication environment. General users do not connect to this schema.

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

Not applicable. The processes have always been centralized in Denver.

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.

General user accounts are used by individuals to retrieve, never to update, the data from the database and the accounts are given access privileges only to the data that is required by the individual to perform their work. Individuals cannot set their own privileges. The privileges required are determined by the data steward for the data; i.e., financial and human resource data stewards work together to determine what data a user typically requires to perform their routine work. Further, general users typically run Corporate reports to retrieve data. The identifiers available to the general users when they generate corporate reports are controlled by the reporting tool's (Impromptu) catalog which is created and maintained by only a small number of Reclamation employees. The Impromptu catalog, along with the privileges set in the Oracle database for the user, then allows the user to retrieve data by the following identifiers:

Individual's name

General users also can connect to the CDW outside of the corporate reporting tool Impromptu; the users still only have access to the data which a data steward has determined they need to perform their work. The personal identifiers available to general users outside of Impromptu are:

Individual's name
Individual's SSN
Vendor ID (equivalent to a Reclamation employee's SSN)
Vendor name (equivalent to a Reclamation employee's name)

Bankcard number (can assist in the retrieval of the individual's name and bank account number)

Database administrators can retrieve data by the following identifiers:

Individual's user account ID (can assist in the retrieval of individual's employee records)

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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

The following types of reports can be produced:

Labor cost charges by name or SSN
Billable rates charges by name or SSN
Salary reports by individual name or SSN
Employee reports by name or SSN
Bankcard charges by name or vendor ID or bankcard number

Database administrators can generate a report of user accounts and privileges assigned to the accounts by name or User ID. These reports would not be accessible to general users of the CDW.

The reports are used by Reclamation employees and contractors to carry out their job duties and responsibilities.

The type of report a user can generate is based on Oracle privileges that grant them read access to the data. Oracle privileges are determined by data stewards who work with the Information System Security Manager to establish the privileges in the database. Database administrators use Oracle roles to facilitate the control of privileges. Each user is granted the appropriate Oracle role which they need for their particular work situation. Changes to the privileges contained in the role are communicated in writing to the System Security Manager and managed through a formal Change Management process.

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*
- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*
- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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.)

Providing information is not voluntary.

- RMSS GSS – N/A
- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*
- IDEAS-PD Major Application – IDEAS-PD contains information about individuals within government vendor data obtained from the vendors themselves. Vendors must enter this data in order to use IDEAS-PD. It is the same data that is in CCR, the federally mandated electronic vendor registry owned by GSA. Only vendors registered in CCR can conduct business with the Federal Government, per the FAC-C 2001-16, FAR Case 2002-18 and FAR Final Rule, October 1, 2003.
- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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?

The system operates from a single, centralized database in Denver that users access via the intranet.

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

Indefinite, at this time. PII information is either updated or new information is added. Data from CDW is backed up to disk, tape and then sent to Iron Mountain.

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?

At this time, no reporting data is removed from the CDW. The retention period of the general user reports, either generated Corporate Reports or ad-hoc reports created by the user, is determined by each user.

Computer media are managed by the Denver Data Center (RMSS) staff and disposed in accordance with Directives and Standards IRM 08-13, *"*Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal." The procedures for the disposition of media are contained in the RMSS Security plan.

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?

N/A.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes, this system provides the ability to:

a. Identify an employee and where the individual is located organizationally;
b. Monitor the types and cost of individual's activities;
c. Monitor employee leave balances.
d. Monitor employee bankcard charges.

7) What kinds of information are collected as a function of the monitoring of individuals?

All time and attendance charges to financial account structures, and employee leave charges, which are associated with an individual's name, SSN, and timestamp are collected and reported. Also, information is collected and reported about an individual's bankcard charges.

- RMSS GSS – N/A

- CDW Major Application – None.

- ETAS Major Application – None. Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – None. Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – None. Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – None. Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – None. Refer to the *ESAM Privacy Impact Assessment*

8) What controls will be used to prevent unauthorized monitoring?

See Operational Controls in the CDW IT System Security Plan.

- RMSS GSS – N/A

- ETAS Major Application – Refer to the *ETAS Privacy Impact Assessment*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Privacy Impact Assessment*

- CARMA Major Application – Refer to the *CARMA Privacy Impact Assessment*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

CDW is covered by the following:
lNTERIOR/DOl-85 - Payroll, Attendance, Retirement, and Leave Records (64 FR 26997, dated 5/18/99).

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No.

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)

Employees, contractors, developers, system and database administrators have limited access based on their roles.

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

Before access is granted to a general user, user access forms are completed through the appropriate routing, including the local Coordinator, CDW Project Manager, and Reclamation Enterprise Service Center. Every general user is granted only those privileges necessary for he/she to complete their responsibilities. Roles are defined in the CDW IT System Security Plan. Procedures have been distributed and documented.

Procedures for creating and maintaining user accounts used to maintain the database are documented in the *Oracle Security SOP, ORA-SOP-011*.

- RMSS GSS – RMSS is a general support system and provides computing resources and network services for other systems and applications. Refer to the documentation for individual systems/applications hosted by RMSS for details regarding access to the data maintained by these systems. Access to RMSS resources is controlled via Active Directory based upon user needs.

- CDW Major Application – Refer to the *CDW Information System Security Plan.*

- ETAS Major Application – Refer to the *ETAS Information System Security Plan*

- IDEAS PD Major Application – Refer to the *IDEAS-PD Information System Security Plan.*

- CARMA Major Application – Refer to the *CARMA Information System Security Plan.*

- TSCMIS Major Application – Refer to the *TSCMIS Privacy Impact Assessment*

- ESAM Major Application – Refer to the *ESAM Privacy Impact Assessment*

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

Every CDW user account is granted only those privileges necessary for he/she to complete their responsibilities.

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)

The CDW limits access based on user accounts and roles. Corporate reports also restrict access to Privacy Act data by hiding the data and not displaying it on the report. Reports that must display Privacy Act data are controlled by granting access to the Privacy Act data to only those users with a need to know the data.

Users are required to sign a CDW Rules of Behavior document which prohibits some specific use and access of the data. In addition, treatment of Privacy Act information is included in the required IT Security Awareness Training.

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. The following Privacy Act Clauses are in the basic Information Technology Omnibus Procurement (ITOP) contract for contractors involved with CDW:

   FAR 52.224.01 Privacy Act Notification
   FAR 52.224.02

   In addition, contractors are only given access on a need to know basis.

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

   Yes, as described in the CDW IT System Security Plan, System Interconnection/Information Sharing Section.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   The system owner and system manager, identified in each IT System Security Plan, is responsible for protecting the Privacy Act data in the interconnected systems.

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?**

   N/A.

10) **Who is responsible for assuring proper use of the data?**

    The Maintenance Services Division, as well as managers and supervisors at Reclamation facilities are responsible for assuring proper use of the data.

    Due to the sensitive nature of the data within the CDW system, the security controls such as "access controls" have been implemented to protect the data. Access controls as defined by NIST SP 800-53 is a mechanism put in place to restrict access to data based on the required authentication and need to know.

Essentially users are able to access only the data for which they are authorized based on their login credentials.

CDW further protects data through active account management, enforcement of assigned authorizations, separation of duties, utilizing the concept of least privilege/functionality, limiting failed access attempts, and prohibiting remote access, among other things. Additionally, included in Reclamation continuous monitoring programs, the above mentioned controls are evaluated regularly by the CDW ISSO.

Continuous Monitoring:
Security controls are monitored throughout the year through annual system assessments, annual ICR review, quarterly updates to the CDW Plan of Action and Milestones (POA&M) and annual review of the CDW System Security Plan and CDW Risk assessment. All system changes must go through the Change Management Process for review, security impact analysis, and approval to determine the impact of the proposed change on the security of the system. The Change Management Process is located at http://intra.do.usbr.gov/itops/rise/rfc/. Documentation and assessment of these system changes become a part of the system record in the overall configuration management process. This system follows NIST Pub 800-37 recommendations for continuous monitoring: Configuration management and control, Security control monitoring, Status reporting and documentation.