

Department of the Interior
Privacy Impact Assessment Template

Name of Project: Reclamation Electronic Document System (REDS)

Bureau: Bureau of Reclamation

Project's Unique ID: 010-10-01-07-1011-00-404-142

A. CONTACT INFORMATION:

Who is the Bureau/Office Privacy Act Officer who reviewed this document?

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual¹¹? Yes

b. Is the information about individual members of the public? No

c. Is the information about employees? Yes

2) What is the purpose of the system/application? REDS manages information in the Bureau of Reclamation through the use of a drawing management component and a records management component:

- The drawing management component provides a workflow for the creation and approval of Reclamation's engineering drawings, including tracking of revisions and version control. The component also provides for storage of electronic drawing files.
- The records management component of REDS provides the capability of indexing physical records and folders to allow ease of locating and retrieving.

¹¹ "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).

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

- National Archives and Records Administration Act of 1984 (P.L. 98-497) 44 U.S.C. Chapter 21 – National Archives and Records Administration
 - Chapter 29 – Records Management by the Archivists of the United States and Administrator of General Services
 - Chapter 31 – Records Management by Federal Agencies
 - Chapter 33 – Disposal of Records
 - Chapter 35 – Coordination of Federal Information Policy
 - Chapter 36 – Management and Promotion of Electronic Government Services
- Electronic Freedom of Information Act Amendments of 1996
- Government Paperwork Elimination Act
- Government Performance and Results Act
- Safety of Dams Act of 1978
- E-Government Act of 2002
- Information Technology Management Reform Act of 1996
- Paperwork Reduction Act
- Freedom of Information Act
- Privacy Act
- 36 CFR Sub-chapter B – Part 1220-1238
- 41 CFR Sub-Chapter C – Part 102 – 193
- Office of Management and Budget Circular A-130 Appendix III – Management of Information Resources
- Office of Management and Budget Circular A-123

C. DATA in the SYSTEM:

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

The categories of individuals are internal Reclamation employees and contractors who are users of the system.

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?**

Both, the REDS User Account form is completed by the individual, who provides the information. Additionally, the information is captured from Active Directory, which also originates from a Network User account form, completed by the individual.

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

Bureau of Reclamation

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

This is not applicable to REDS.

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

This is not applicable to REDS.

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

The Reclamation employee or internal contractor who is a user of the REDS has their first name and last name entered into the system. There is no information collected from the public.

3) Accuracy, Timeliness, and Reliability

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

None of their data is collected.

- b. **How will data be checked for completeness?**

Data integrity is checked by the individual's Supervisor and the Reclamation Records and Drawings Managers through the approval process of the REDS User account form. It is also checked for completeness against Active Directory. This will ensure that only current and authorized users have access to the REDS.

- c. **Is the data current?**

Yes.

- d. **Are the data elements described in detail and documented?** N/A

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. Individuals must have an approved user account to access the REDS for search, read/write access.

- 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 it will not. This is not applicable to REDS.

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

No it will not. This is not applicable to REDS.

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

No it cannot. This is not applicable to REDS.

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

Internal Reclamation employees and approved contractors seeking access to the system must complete a User Account form, which is reviewed and approved by the Records or Drawing Manager. The user's first name and last name will also be verified via integration with Active Directory.

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

User Authentication with Active Directory, and REDS user groups, roles and permissions are the controls that are in place to prevent unauthorized access to the system and data.

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

User Accounts are centrally managed in the Denver Office by the System Security Manager in collaboration and cooperation with the RESC Support Team and the AD Administrators.

- 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.**

A Search can be performed on the internal Reclamation employee's first name, last name, or combination.

- 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 REDS Reports that can be produced on individuals can:

1. Report the actions of the internal Reclamation employee, such as records/folders added, modified, or deleted.
2. Which sites/locations that the individual has access to.
3. What permissions the individual has.

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.)

REDS User Account forms are necessary to meet the auditing and accountability and access control requirements for IT system security. The REDS is integrated with Active Directory and there is no way to decline providing first name/last name in conjunction with a network account.

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?

REDS configuration is maintained in Denver and data for REDS is stored only in Denver. The User Account forms are maintained in Denver by the ISSO.

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

REDS User account forms are closed at the end of the calendar year in which access has been superseded, revoked, or employee has transferred or separated from service.

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?

The REDS User Account forms are destroyed in agency one year after closure.

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?

This is not applicable to REDS.

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

No

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

This is not applicable to REDS.

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

This is not applicable to REDS.

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

Payroll, Attendance, Retirement, and Leave Records--Interior, DOI--85.

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

N/A

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)

Bureau of Reclamation employees and contractors with the need to manage records and drawings.

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

User access is approved by supervisors and records and drawings managers, and documented on user access forms along with their level of access to the system.

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

User access is restricted by the use of roles and groups and permissions assigned to each, within the system.

- 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)**

Guidance on the proper use of the REDS can be found in:

REDS Records Management User Guide

REDS Training Manual

REDS Drawings Help Screen

- 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, contractors are involved with REDS and all contracts have Privacy Act clauses.

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

No

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

N/A

- 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?**

This is not applicable to REDS.

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

REDS System Admins, ISSO, RESC Support.