Reclamation Manual

Directives and Standards

Subject: Privacy and Safeguarding Personally Identifiable Information (PII)

Purpose: This Directive and Standard (D&S) describes the procedures and responsibilities governing the privacy of information relating to employees, contractors, customers or other individuals and the release, protection, and management of Bureau of Reclamation records. The benefits of this D&S are the compliance with the Privacy Act of 1974, as amended.

Authority: The Privacy Act of 1974, as amended, 5 U.S.C. § 552a; E-Government Act of 2002, Section 208 – Privacy Provisions; Federal Information Security Modernization Act of 2014 (FISMA); 5 CFR § 293.211, Availability of Information; 43 CFR Part 2, Subpart K, Privacy Act; 383 Departmental Manual Chapters 1-13; National Institute of Standards and Technology (NIST) SP 800-53 (Rev 4); NIST SP 800-122; Office of Management and Budget (OMB) OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information; OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services; OMB M-10-23, Guidance for Agency Use of Third-party Websites and Applications; OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies; OMB Circular A-130 Revised "Managing Information as a Strategic Resource"; OMB Circular A-108 "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act"; DOI Privacy Breach Response Plan; the DOI Privacy Impact Assessment Guide; DOI Privacy Threshold Analysis Guide; Departmental Manual Chapter 24, Parts 112, 212 and 375; and Departmental Manual Chapter 4, Part 36.

Approving Official: Associate Chief Information Officer (ACIO), Information Resources Office (IRO)

Contact: Information Resources Office, 84-21000

1. **Introduction.** The Privacy Act establishes special requirements for the creation, maintenance, dissemination, and protection of records that contain PII. The objectives of the Bureau Privacy program are to ensure compliance with the Privacy Act of 1974, as amended, and the E-Government Act of 2002 for the maintenance and protection of records that contain information about individuals. In addition, it follows the requirements established by NIST, OMB, and the Department of the Interior to safeguard and protect PII, conduct privacy threshold analysis', privacy impact assessments, and report privacy breaches involving confirmed or suspected breaches of PII.

2. **Applicability.** This D&S applies to all Reclamation employees and staff, temporary, volunteer, and permanent, as well as customers or other individuals.

3. **Definitions.**

A. **Breach.** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. Examples include, but are not limited to:

(1) a laptop or portable storage device storing PII is lost or stolen;

(2) an email containing PII is inadvertently sent to the wrong individual;

(3) a box of documents with PII is lost or stolen during shipping;

(4) an unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;

(5) a user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;

(6) an IT system that maintains PII is accessed by a malicious actor; or

(7) PII that should not be widely disseminated is posted inadvertently on a public website.

B. **Disclosure.** The release of information contained in a system of records to any person (other than the person to whom the information pertains), including any employee of Reclamation, the Department, or employees of other Federal departments and agencies.

C. **Incident.** An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

D. **Maintain.** The collection, use, or dissemination of records about individuals.

E. **PII.** PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

(1) Sensitive PII, which if lost, compromised, or inappropriately disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

(2) Sensitive PII has stricter handling requirements. Some PII is not sensitive such as information found on a business card or official email signature block. This type of non-sensitive PII generally does not require special handling.

(3) The context of the PII should must be considered to determine its sensitivity, such as a list of employees with poor performance ratings as opposed to a list of employees who completed privacy training. Note that even when an individual's name is not present it may still be PII if it can be used to identify or be linked to an individual, and PII can also be created when information about an individual is made available or combined with other information.

(4) Examples of Sensitive PII include:

(a) name, such as full name, maiden name, mother's maiden name, username, or alias;

(b) personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;

(c) partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual;

(d) address information, such as personal mailing address or personal email address;

(e) asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;

(f) personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);

(g) information identifying personally owned property, such as vehicle registration number or title number and related information; and

(h) information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

F. **Privacy Impact Assessment (PIA).** PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

G. **Privacy Threshold Analysis (PTA).** PTA is a tool used by the Associate Privacy Officer (APO) in collaboration with the Information System Security Officer and subject matter experts to (1) identify programs, projects, information collections and information systems that are privacy-sensitive, (2) determine requirements for a PIA, Adapted PIA, or additional privacy compliance requirements for the collection, maintenance, use, processing, sharing or disposal of PII, (3) demonstrate that privacy considerations were included during the review of a program, project, information collection or information system, (4) provide a record of determination of privacy requirements for the program, project, collection or information system for the Program Official, System Owner and the Privacy Office, and (5) demonstrate compliance with privacy laws, regulations and policy.

H. **Routine Use.** An authorized disclosure outside of the Department, which is published in an applicable Privacy Act System of Record.

I. **System of Records.** A group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier assigned to the individual.

J. **System of Records Notice (SORN).** Published in the Federal Register and describes a system of records subject to the Privacy Act to include: the system name and number; security classification; system manager; statutory authority for maintenance of the system; purpose(s) of the system; categories of individuals; categories of records; record source categories; routine uses; policies and practices for storage, retrieval, retention and disposal of records; administrative, technical and physical safeguards; and records access procedures.

4. **Responsibilities.**

A. **ACIO.** The ACIO has overall responsibility for ensuring compliance with all applicable regulatory, statutory, Federal, and Departmental requirements.

B. **APO.** The APO carries out the responsibility of the ACIO for implementing privacy requirements and will:

(1) manage and administer the Bureau Privacy program;

(2) implement policies, processes, and procedures for privacy;

(3) provide guidance to regions, directorates and offices to meet the requirements of this policy:

(a) to identify and address information privacy practices during the system lifecycle, e.g., planning, developing, implementing, and operating of systems used by the Bureau that maintain information on individuals;

(b) to assist when preparing and reviewing privacy compliance documentation for Departmental approval;

(c) to limit access to and disclosure of PII to personnel with an official need to know in order to accomplish an official mission, administrative function, or statutory requirement;

(d) to ensure appropriate safeguards are applied to all information about individuals; and

(e) to reduce unnecessary collections of social security numbers and limit its use to only those instances specifically authorized by law;

(4) manage, review, and update the Bureau inventory of SORNs and PIAs;

(5) prepare and consolidate the Reclamation-wide annual FISMA report and other Privacy reports in response to all Departmental data calls;

(6) provide assistance, guidance, and training to Privacy Act Coordinators and program offices maintaining system of records covered by the Privacy Act;

(7) conduct on-site assessments bi-annually of regional offices, Denver directorate offices, and any other office as needed or requested by the regions where records subject to the Privacy Act are maintained;

(8) interpret and disseminate Departmental guidelines/directives;

(9) establish, maintain, and revise system of records notices for all systems of records;

(10) coordinate, investigate, remediate, mitigate and track confirmed and suspected privacy breaches in accordance with the DOI Privacy Breach Response Plan;

(11) coordinate assignment, notification, tracking, and completion of annual privacy awareness and role-based training by Bureau personnel;

(12) study issues related to privacy trends and the application to procedures and processes used by Reclamation programs; and,

(13) attend events and engage in working groups sponsored by the Federal Privacy Council and Departmental Privacy Office, among others.

C. **Regional Privacy Coordinators.** Regional Privacy Coordinators are responsible for overseeing the implementation of privacy requirements in their regions and will:

(1) provide guidance to program, area and field offices to meet the requirements of this D&S;

(2) respond to written requests for records covered by the Privacy Act, and coordinate denials with the Office of the Solicitor and the APO;

(3) conduct on-site assessments of regional area and field offices or send out the Privacy Assessment Checklist (see Appendix B) bi-annually to area and field offices for self-assessments;

(4) conduct program office assessments located at the regional office as needed or requested by the program office where records subject to the Privacy Act are maintained;

(5) provide training and guidance to program, area, and field offices maintaining systems of records covered by the Privacy Act as requested;

(6) collaborate with APO on tracking and completion of annual privacy awareness and role-based training by regional personnel;

(7) collaborate with APO on coordinating, managing, and tracking privacy breach activities in accordance with the Department Breach Response Plan for confirmed or suspected breaches of PII maintained by the program, area, or field offices through mitigation and lessons learned activities;

(8) provide input to reports and data calls as requested by the APO; and

(9) review and coordinate all regional PTAs and PIAs with the APO.

D. **Privacy Act System Owners/Managers.** Privacy Act system owners/managers are responsible for:

(1) ensuring that the information collected and maintained in hardcopy or an information management system conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) ensuring that this D&S is implemented for their systems in consultation with the Privacy Office; and

(3) reporting any privacy breaches confirmed or suspected to their supervisor, APO and Regional Privacy Coordinator within one hour of discovery.

E. **Managers/Supervisors.** Managers/supervisors are responsible for:

(1) ensuring this D&S is implemented and enforced;

(2) informing employees, contractors, volunteers and all persons performing work for Reclamation of this policy as it relates to activities within the scope of the supervisor's responsibility; and

(3) reporting any privacy breaches confirmed or suspected to the APO and Regional Privacy Coordinator within one hour of discovery.

F. **Employees and All Other Personnel.**

(1) All Reclamation employees who are involved in the maintenance of records subject to the Privacy Act must comply with the provisions of the Privacy Act and must adhere to all Federal and Departmental privacy requirements.

(2) Employees and all other personnel are responsible for:

(a) reporting any breaches of confirmed or suspected PII breaches to their manager/supervisor, APO, and Regional Privacy Coordinator within 1 hour of discovery; and

(b) completing all mandatory privacy training requirements.

5. **Requirements.**

A. **Handling PII.** Exercise care when handling all PII. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised.

(1) **Disposing of Sensitive PII.** Sensitive PII, including that found in archived emails must be disposed of when no longer required, consistent with the applicable records disposition schedules. If destruction is required, take the following steps:

(a) Shred paper containing sensitive PII using an approved cross-cut shredder (NIST SP 800-88 revision 1, Appendix A. Minimum Sanitization Recommendation for Media Containing Data); do not recycle or place PII in garbage containers. Companies who supply secure shred bins are acceptable.

(b) Before transferring your computer or any other devices to another employee, the IT Help Desk must sanitize sensitive PII from computer drives and other electronic storage devices.

(2) **Emailing Sensitive PII Within the Department's Network.** PII may be emailed to a recipient with an official need to know within the Department/Reclamation network as it is properly encrypted with-in the Department's environment. However, unencrypted PII creates a risk of unauthorized disclosure, especially when employees use the auto forward feature, reply to all, or forward to unintended recipients. As a best practice, individuals must redact, password protect, or encrypt sensitive PII when emailing within the Department's network to protect sensitive PII and mitigate the risk of a privacy breach. Before emailing sensitive PII within the Department's network, confirm that you have the correct email address and always ensure the recipient is authorized to access and view the sensitive PII.

(3) **Emailing Sensitive PII Outside the Department Network.** When emailing sensitive PII outside the Department's network, individuals are required to encrypt any attachment that contains sensitive PII and provide the password separately to the recipient by phone, email, or in person. Always confirm that you have the correct email address and ensure the recipient is authorized to access and view the sensitive PII.

(4) **Emailing Sensitive PII to Personal Accounts.** Never email sensitive PII to personal email accounts or forward government email containing sensitive PII to personal accounts. Personal email accounts may not be used to transmit or receive sensitive PII. Sensitive PII may only be transmitted on the Department's network. Personal computers may not be used to access, save, store, or host sensitive PII.

(5) **Network Drives and Collaboration Systems.** Owners of network drives, shared network drives and collaboration systems including but not limited to SharePoint and Google Drive are required to ensure that appropriate security and privacy controls are in place to limit access to authorized users and to encrypt folders when possible, if there is an official need to post sensitive PII to those systems. Audits of these systems are to be conducted, at a minimum, annually by the owners of the network and shared network drives and the data owners of the collaboration systems to review and verify authorized user access and the continued need for maintaining sensitive PII on those drives systems.

B. **Collecting Information from Employees, Contractors, or Other Individuals.**

(1) **Collection.** Reclamation may only collect and maintain information relating to individuals that is needed or relevant to carry out a purpose authorized by statute or by executive order. To the greatest extent practical, information will be

collected directly from the individual. Reclamation may not collect or maintain information describing how individuals exercise their rights protected by the First Amendment. The only exceptions to this restriction are when the maintenance of such information is specifically authorized by statute or by the individual about whom the record is maintained or it pertinent to and within the scope of an authorized law enforcement activity.

(2) **Notice.** When Reclamation asks individuals to provide information about themselves and that information is maintained in a system of records, Reclamation must provide an appropriate privacy notice. The Reclamation APO must approve all forms (hardcopy and electronic) that collect this information, this includes surveys.

(3) **Choice.** When individuals provide their information, when they register for, or request a product or service, and Reclamation maintains the information in a system of record, individuals must be given a choice as to whether the information may be used for a secondary use such as marketing a different service.

C. **Managing Information Relating to Employees, Contractors, or Other Individuals.**

(1) **Managing a System of Records.**

(a) The requirements of the Privacy Act of 1974, as amended, must be followed prior to Reclamation maintaining records about individuals which are retrieved by a person's name or other personal identifier.

(b) When Reclamation maintains information about individuals in a system of records, a System of Records Notice (SORN) must be authorized by the Departmental Privacy Officer (DPO) for publication in the Federal Register in accordance with the Privacy Act of 1974, OMB Circular A-108, and Departmental policy. Reclamation may use a Government-wide or Department-wide SORN if it accurately describes Reclamation's system of records, otherwise, a Reclamation specific SORN must be drafted for DPO authorization.

(2) **Create, Modify, or Rescind a SORN.** Employees or managers must notify their regional Privacy Coordinator if they are maintaining information about individuals in a system of records that is not authorized. The regional Privacy Coordinator will notify the APO and collaborate with the APO on creating, modifying, or rescinding a SORN if the SORN pertains only to that region. The APO manages Reclamation's part of the process for creating, modifying, or rescinding an authorized system of records prior to submission to the DPO. The DPO reviews, approves, and surnames the SORN at the Department level and

then forwards the notice to Congress and OMB for comment prior to publication to the Federal Register. Once published in the Federal Register, the SORN goes into effect allowing the collection of PII with the exception of the routine uses. The public has 30 days to comment on the proposed routine uses; if there are no comments of significance which would require a change to the proposed routine use, the routine uses go into effect after the 30-day period.

(3) **Continuous Monitoring.** The manager(s) of an IT system must notify the APO if changes are planned to a program or a system which may require the authorized SORN to be modified. At a minimum, a SORN must be reviewed every two years to ensure that it is still accurate and complete.

(4) **Official Inventory of SORNs.** The DPO maintains the official Department inventory of SORNs on the Department SORN webpage. Links to SORNs must be directed to the official inventory.

(5) **Section 508 Compliance.** The Rehabilitation Act of 1973 requires Federal agencies to make their electronic and information technology accessible to people with disabilities. Agencies must give employees with disabilities and members of the public access to information that is comparable to the access available to others. All approved and signed SORNs must be made 508 compliant prior to submitting to the DPO for posting in the Department's official SORN inventory.

D. **PTA.** PTA are to be completed at the earliest stages of the information lifecycle and PIA process to help Reclamation Privacy Officials identify PIA and other privacy compliance requirements for any activities that may have privacy implications in order to take appropriate actions as required under applicable privacy laws, regulations, policies and standards. The PTA is an important tool that helps identify privacy sensitive projects, programs and systems, and identify potential gaps in privacy compliance during the earliest stages of a project, program or system and take appropriate corrective actions. Program Officials and System Owners are responsible for completing the PTA and submitting the PTA to the Reclamation APO for review and a privacy compliance determination.

E. **PIA.**

(1) The PIA is an analysis of how information is handled, or specifically it is an assessment of how PII is collected, used, maintained and disseminated. The PIA is an important tool used to identify evaluate and analyze potential privacy risks associated with the development or use of information systems or applications. The PIA allows Reclamation to evaluate privacy risks, ensure the protection of privacy information, and consider privacy and security implications throughout the life cycle of the system or application. Reclamation may use a

Department-wide PIA if it accurately describes Reclamation's information collection and practices, otherwise, a Reclamation specific PIA will be completed and approved by the DPO.

(2) Program Officials and System Owners are responsible for completing the PIA in collaboration with the Information System Security Officer, the Bureau/Regional Records Officer, the Bureau/Regional Privacy Officer, and the Departmental Privacy Office to ensure potential privacy risks are addressed and appropriate privacy protections are implemented.

(3) Employees or managers must notify the APO if they are maintaining information about individuals in electronic form. The APO, in collaboration with the IT Risk and Portfolio Management Division, manages Reclamation's process for creating, revising, or decommissioning a PIA that will be approved by the DPO.

(4) The manager(s) of electronic collections of personal information must notify the APO if changes are planned which may necessitate revising its PIA. At a minimum, a PIA is required to be reviewed annually as part of IT continuous monitoring and renewed whenever there is a significant change or modification to the system. Official Inventory of PIAs. The DPO maintains the official Department inventory of PIAs on the Department's PIA webpage. Links to Reclamation PIAs must be directed to the official inventory. Section 508 Compliance. All approved and signed PIAs must be made 508 compliant prior to submitting to the DPO for posting in the official inventory.

F. **Disclosing Employee, Contractor, or Other Individuals' Information.**

(1) **Limitation.** Information about individuals contained in a system of records cannot be released to a third party, including a spouse, except as followed under this section.

(2) **Internal Disclosures.** Information may only be disclosed to a Department or Reclamation employee or employee of a contractor managing a Department or Reclamation system of records who has a need to know in the performance of their official duties. Internal disclosures is the first of 12 statutory disclosures allowed under the Privacy Act.

(3) **External Disclosures.** Information may only be disclosed externally under one of four conditions:

(a) Consent – when the individual has authorized the disclosure in writing.

(b) Statute – the disclosure fits within one of the 12 categories listed in the Privacy Act, see 383 DM Chapter 7, Section 7.2, Disclosure Provisions.

(c) Routine Use – one of the 12 categories listed in the Privacy Act. The system of records has established a routine use authorizing disclosure of the record outside of the agency for a purpose which is compatible with the purpose for which it was collected.

(d) Publicly Available – 5 CFR § 293.311 makes certain data about most present and former Federal employees available to the public and may be released: Name, present and past titles, grades, annual salary including awards and bonuses, and work location.

(4) **Accounting of Disclosures.** The Privacy Act requires that records be kept on disclosures to accurately account for every disclosure of information about an individual covered by a system of record, even if the disclosure is made at the individual's request. Records custodians and Privacy Act system managers are to use the Disclosure Account Form DI-3710, Attachment A, for this purpose.

(5) **Exceptions.** The only exceptions to the accounting of disclosures are when the information is disclosed to Department employees in the performance of their official duties; information is disclosed to the individual to whom the information pertains; information released under the Freedom of Information Act; or information that is publicly available.

G. **Handling Breaches of Personally Identifiable Information.**

(1) **Reporting.** All suspected or confirmed breaches of information about individuals must be immediately reported to the APO within one hour of discovery and include a completed DOI Privacy Breach Report, Appendix A. If the APO cannot be reached, immediately report the incident to privacy@usbr.gov. The report of the breach is made by the person who committed the breach or who witnessed the breach with a copy to the person's manager or supervisor. DO NOT include the actual PII in the report as this would constitute another breach.

(2) **Curiosity Browsing.** Individuals with access to sensitive data may only access that data when there is an official need to know. Accessing records when there is no official need constitutes a breach and must be reported.

(3) **Bureau Privacy Breach Response Team.** The Privacy Breach Response Team's purpose is to manage confirmed and suspected breaches of PII at the bureau level. The team is responsible for implementing the DOI Privacy Breach Response Plan; defining policies and procedures for breaches within the control of Reclamation; managing and mitigating breaches based on the risks to the individuals and Reclamation; and advising Reclamation leadership about the team's activities when the team is convened to respond to a breach.

(4) **Mitigating a Breach.** The Reclamation office or division responsible for the breach will be provided guidance to mitigate the breach and must fund any costs associated to mitigating the breach. This may include notification letters to the affected individuals, credit monitoring and/or identity theft protection services, among others.

H. **Training.**

(1) **Privacy Awareness.** All employees, contractors, and other individuals with access to Department and Reclamation's computing network are required to complete mandatory privacy awareness training annually.

(2) **Role-based Training.** Individuals with access to sensitive PII may also be required to take the annual role-based privacy training.

I. **Managing External Web Pages and Emails.**

(1) **Link to Privacy Policy.** All webpages, including those managed by contractors operating on behalf of Reclamation, must conform to current OMB guidance and Department requirements. A link to the Reclamation privacy policy must appear in the footer of every page regardless of whether information is collected from individuals. Pages directed to children under the age of 13 years old must have a link to the Department's Children's Privacy Policy.

(2) **Emails.** Individuals may register to request information from Reclamation for its product or service offerings, e.g., newsletters and training; this is called "Opting In". Contact information may not be used to send emails for other products or services. A link to unsubscribe, or "Opt Out" from emails must be available at the bottom of any message and be honored within 10 business days.

J. **Applying Privacy to Contracts.**

(1) **Access to Information about Individuals.** Contracts must include appropriate privacy and security contract clauses when the contractor has access to information relating to employees, contractors or other individuals.

(2) **Reviews.** The APO will conduct random reviews of Reclamation contracts that provide for the maintenance of a system of records on behalf of Reclamation to ensure the requirements of the Privacy Act apply.

K. **Assuring Integrity of Privacy Act Records.**

(1) Areas in which the records are maintained or regularly used shall be posted with an appropriate warning stating that access to the records is limited to authorized persons. The warning also shall summarize the requirements of 43 CFR § 2.226

and state that the Privacy Act contains a criminal penalty for the unauthorized disclosure of records to which it applies. Areas where the notice is to be posted include but are not limited to, individual file drawers, manager/supervisor offices, doors to program areas, individual sections of rolling/electronic filing systems, etc. Only areas that contain privacy act information are to be labeled.

(2) During working hours:

(a) the area in which the records are maintained or regularly used shall be occupied by authorized personnel, or

(b) access to the records shall be restricted by their storage in locked file cabinets or a locked room.

(3) During non-working hours, access to the records shall be restricted by their storage in locked file cabinets or a locked room.

(4) Where a locked room is the method of security provided for a system, the bureau responsible for the system shall supplement that security by (i) providing lockable file cabinets or containers for the records or (ii) changing the lock or locks for the room so that they may not be opened with a master key. For the purposes of this paragraph, a master key is a key which may be used to open rooms other than the room containing records subject to the Privacy Act, unless those rooms are utilized by officials or employees authorized to have access to the records subject to the Privacy Act.

RECLAMATION
Managing Water in the West

RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: _____ Release No. **101**

Ensure all employees needing this information are provided a copy of this release.

Reclamation Manual Release Number and Subject

RCD 01-02 Privacy and Safeguarding Personally Identifiable Information (PII)

Summary of Changes

Minor revisions approved to reflect Department of the Interior requirements and align Reclamation with the following:

- **OMB Circular A-130 Revised "Managing Information as a Strategic Resource"**
- **OMB Circular A-108 "federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act"**
- **OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information**
- **OMB M-l7-06, Policies for federal Agency Use of Third-party Websites and Applications**
- **National Institute of Standards and Technology SP 800-53 (Rev 4) and SP 800-122**
- **DOl Privacy Breach Response Plan**
- **DOl Privacy Impact Assessment Guide**
- **DOl Privacy Threshold Analysis Guide**

NOTE: This Reclamation Manual release applies to all Reclamation employees. When an exclusive bargaining unit exists, changes to this release may be subject to the provisions of collective bargaining agreements.

Filing instructions

Remove Sheets	Insert Sheets
RCD 01-02 pp 1-4	**RCD 01-02 pp 1-14** **Appendix A pp 1-5** **Appendix B pp 1-3**

All Reclamation Manual releases are available at http://www.usbr.gov/recman/

Filed by: _____ Date: _____