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 Privacy Act records. The benefits of this D&S are the compliance with the Privacy Act of 1974, as amended and improved internal and external collaboration, communication, and consistency in handling PII.

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; 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 (DM) 112 DM 24, 212 DM 24, 375 DM, 383 DM 1-13Departmental Manual..

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

Contact: Risk Management Services Division, Enterprise Security Operations (84-21310)

1. **Introduction.** The Privacy Act establishes special requirements for the creation, maintenance, dissemination, and protection of records that contain PII. The objectives of the Reclamation 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 analyses, privacy impact assessments, and report privacy breaches involving confirmed or suspected breaches of PII.

2. **Applicability.** This D&S applies to all Reclamation employees (i.e., temporary, volunteer, and permanent).

3. **Program Management.**

A. The ACIO will ensure compliance with all applicable privacy regulatory, statutory, Federal, and Departmental requirements.

B. The Associate Privacy Officer (APO) will carry out the responsibility of the ACIO for implementing privacy requirements across Reclamation.

C. Regional privacy coordinators will implement privacy requirements for their respective regions.

D. Privacy Act system owners/managers will ensure that information collected and maintained regardless of media conforms to applicable legal, regulatory, and policy requirements regarding privacy.

E. Managers and supervisors must inform employees of the existence and location of the Reclamation Manual and their responsibility for understanding and adhering to this D&S.

4. **Requirements.**

A. **Handling PII.** All employees must 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.** Employees must dispose of sensitive PII, including that found in archived emails, when it is no longer required consistent with the applicable records disposition schedules. If destruction is required, employees must 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 information technology (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. Employees 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, employees must confirm they 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's Network.** When emailing sensitive PII outside the Department's network, employees are required to encrypt any attachment that contains sensitive PII and provide the password separately to the recipient by phone, email, or in person. Employees must always confirm they 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.** Employees shall not email sensitive PII to personal email accounts or forward government email containing sensitive PII to personal accounts unless it is encrypted and it's their own PII. Personal email accounts shall not be used to transmit or receive sensitive PII for government purposes. Sensitive PII must only be transmitted on the Department's network. Personal computers shall not be used to access, save, store, or host sensitive PII collected for business purposes.

(5) **Network Drives and Collaboration Systems.** Owners of network drives, shared network drives, and collaboration systems including but not limited to SharePoint, One Drive, and Teams 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. Owners of the network and shared network drives and the data owners of the collaboration systems are required to conduct audits of these systems at a minimum, annually to review and verify authorized user access and the continued need for maintaining sensitive PII on those drives and systems.

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

(1) **Collection.** Reclamation must only collect and maintain information relating to individuals that is needed or relevant to carry out a purpose authorized by statute or executive order. To the greatest extent practical, employees must collect the information directly from the individual. Reclamation must 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 is 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 and surveys (hardcopy and electronic) that collect this information.

(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, Reclamation must provide the individuals a choice of 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) Employees must follow the requirements of the Privacy Act of 1974, as amended, 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 uses, 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 2 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 website. 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. Reclamation 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 508 compliant prior to submitting to the DPO for posting in the Department's official SORN inventory.

D. **Privacy Threshold Analysis (PTA).** Program managers, system owners and information system security officers must complete and submit a PTA to the APO for review and approval at the earliest stages of the information lifecycle and privacy impact assessment (PIA) process to help the APO and the regional privacy coordinator 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. Program officials and system owners must complete and submit 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 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 by the program manager, system owner, and the information system security officer in collaboration with the APO and approved by the DPO.

(2) Program managers and system owners must complete the PIA in collaboration with the information system security officer, the Reclamation/regional records officer, the APO and/or the regional privacy coordinator, 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 Information Management and Technology Service Strategy 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 or every 3 years.

(5) **Official Inventory of PIAs.** The DPO maintains the official Department inventory of PIAs on the Department's PIA website. Links to Reclamation PIAs must be directed to the official inventory. The APO will make all approved and signed PIAs 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.** Employees must only disclose information 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 disclosure is the first of 12 statutory disclosures allowed under the Privacy Act.

(3) **External Disclosures.** Employees must only disclose information 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 employees to keep records on disclosures to accurately account for every disclosure of information about an individual covered by a system of record, even if the disclosure is 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 PII.**

(1) **Reporting.** Employees must immediately report all suspected or confirmed breaches of information about individuals to the APO within 1 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. Employees must NOT include the actual PII in the report as this would constitute another breach.

(2) **Curiosity Browsing.** Individuals with access to sensitive data must 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 convenes to respond to a breach.

(4) **Mitigating a Breach.** The APO or the regional privacy coordinator will provide guidance to the Reclamation office or division responsible for the breach to mitigate the breach. The Reclamation office or division responsible for the breach must fund any costs associated to mitigating the breach (e.g., notification letters to the affected individuals, credit monitoring and/or identity theft protection services).

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 Websites and Emails.**

(1) **Link to Privacy Policy.** All websites, 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. Websites 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." Employees must not use contact information 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.** Employees must ensure that contracts 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) Employees will ensure areas in which the records are maintained or regularly used are posted with an appropriate warning stating that access to the records is limited to authorized persons. The warning shall also 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.

L. **Privacy Compliance Assessments.**

(1) The regional privacy coordinators will conduct on-site privacy assessments or virtual privacy assessments using the checklist in Appendix B, for area and field offices every 3 years.

(2) The APO will conduct on-site privacy assessments or virtual privacy assessments using the checklist in Appendix B for the regional offices and the Denver directorate offices every 3 years.

5. **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. **Personally Identifiable Information or PII.** 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 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 (i.e., IP) or Media Access Control (i.e., 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 or PIA.** 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 or PTA.** A tool used by the 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 or 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.

6. **Review Period.** The originating office will review this release every 3 years.

RECLAMATION
Managing Water in the West

RECLAMATION MANUAL TRANSMITTAL SHEET

Effective Date: **03/31/2022** 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

1.
revisions to comply with RM format, and
2.
minor grammatical and editorial revisions.

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 1-14	**RCD 01-02 pp 1-12**
Appendix A pp 1-5	**Appendix A pp 1-5**
Appendix B pp 1-3	**Appendix B pp 1-3**

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

Filed by: **Marciano Budel** Date: **03/31/2022**