Reclamation Manual

Policy

Subject: Reclamation Information Technology Security Program

Purpose: Defines and establishes authorities, principles, responsibilities, and accountability for Reclamation Information Technology Security Program.

Authority: The Privacy Act of 1974; Federal Managers' Financial Integrity Act of 1983; Public Law 100-235, The Computer Security Act of 1987; National Defense Authorization Act for Fiscal Year 2001 (Subtitle G–Government Information Security Reform); OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*; OMB Circular A-123, *Internal Control Systems*; CIAO Practices for Securing Critical Information Assets (January 2000); and Department of the Interior Departmental Manual Part 375 Chapter 19.

Contact: Information Resources Services, D-7100

1. **Purpose.** Reclamation's Information Technology (IT) systems are a vital part of the infrastructure supporting the agency's mission of managing, developing, and protecting water and related resources in an environmentally and economically sound manner. These IT systems are protected from threats so that Reclamation can maintain and monitor contract obligations, safely and reliably operate facilities, and carry out mission-related administrative support responsibilities.

2. **Definitions.**

   A. **Information Technology (IT).** The equipment, interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. The term includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

   B. **IT Threat.** A physical, electrical, or information-based hazard or compromise to an IT system or the communications, information, or control activities it performs or to which it is connected.

   C. **Trusted.** Confidence that an interfacing system, user, or network has met Reclamation requirements and will not compromise, corrupt, interrupt, change, or harm a Reclamation IT system or network. Untrusted means a lack of confidence, or of unknown confidence.

3. **Goals and Objectives.**

A. Reclamation's IT Security Program will:

(1) Ensure the safety of personnel and the public.

(2) Protect the Federal investment.

(3) Take all reasonable and prudent precaution to prevent IT threats from detrimentally impacting mission effectiveness.

(4) Ensure the integrity of IT services to authorized project beneficiaries by determining acceptable risk levels and by conducting periodic IT system audits to ensure compliance.

(5) Provide for timely delivery of services via IT.

4. **Principles.**

A. Reclamation's Information Technology Security Program (IT Security Program) incorporates security into the business practices and architecture of Reclamation's IT systems. The business requirement of protecting IT systems includes determination of acceptable risk and cost benefit analyses of alternative solutions. IT Security Program performance is measured to ensure IT system security cost-effectively supports Reclamation's mission.

B. Electronic information is managed and protected as a Reclamation-wide asset. The IT Security Program includes electronic Information Sensitivity Directives and Standards in order to support required asset management and implement appropriate protective procedures.

C. The IT Security Program incorporates efficient and effective Configuration Management Directives and Standards designed to ensure that system, procedural, organizational, physical, and personnel changes do not threaten IT system operations or increase vulnerabilities or risks.

D. The IT Security Program enforces a network security perimeter for IT systems as defined in the Network Systems Directive and Standard. These Directives and Standards identify the protective mechanisms to be implemented with trusted and untrusted systems and users.

E. IT security training and awareness is a Reclamation priority. The IT Security Program requires adequate IT security training for users, managers, IT technical personnel, and IT security personnel.

5. **Scope.** This policy and the supporting Directives and Standards apply to:

A. All Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., SCADA, Hydromet, GIS, Dam Safety).

B. All Reclamation-owned IT systems operated and/or maintained by contract or temporary personnel.

C. All Reclamation-owned IT systems operated and/or maintained by organizations or personnel other than Reclamation.

6. **Responsibility/Accountability.**

A. Reclamation's Chief Information Officer (CIO) is responsible and accountable for leading the IT Security Program and reports directly to the Commissioner of Reclamation.

B. Reclamation Directors, managers, and employees are responsible and accountable for ensuring systems are designed, implemented, and maintained in accordance with the IT Security Program Policies, Directives and Standards, and guidelines. Directors and managers are responsible for keeping the CIO adequately informed of IT Security Program issues, decisions, and accomplishments.

7. **Supporting Directives and Standards.** Reclamation Manual Directives and Standards necessary to define the procedures and minimum mandated standards of practice for the IT Security Program will be developed in a collaborated process with input from affected managers and user communities and issued under the direction of Reclamation's CIO and included in the IRM section of the Reclamation Manual.