Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Physical Controls for IT

Purpose: Defines physical access, building, storage, and security parameters for the protection of Reclamation data and other IT resources.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 25, 1985); OMB Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); OMB Circular No. A-127, *Financial Management Systems*; The Computer Security Act of 1987 (Public Law 100-235); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (January 2000); Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*; DM Part 441, *Personnel Security and Suitability Requirements*; and Presidential Decision Directive 63, *Critical Infrastructure Protection*, May 1998.

Contact: Information Resources Services, D-7100

1. **Introduction.** This Directive and Standard describes requirements for minimal physical protection of Reclamation IT resources.

2. **Goals.**

   A. Describe minimal access control for the protection of Reclamation IT resources.

   B. Define requirements for physical structures, locations, and internal areas where Reclamation restricted/sensitive data may be generated and/or stored.

   C. Protect IT installations from theft, vandalism, accidents, and other disasters.

3. **Definitions.**

   A. **IT Equipment.** For the purpose of this document, IT equipment includes shared computers (e.g., servers), peripherals, and telecommunications equipment.

   B. **Restricted Data.** Information/data, including that received from external sources, requiring the highest level of "Access Control" protections based on the extent of harm caused by its unauthorized, inadvertent, or deliberate disclosure, alteration, use, or destruction. Such

improper use, modification, or disclosure would adversely affect Reclamation business partners, customers, and employees, and the agency's ability to accomplish its mission, safeguard the public, and protect the legal and financial rights of the Federal Government.

C. **Sensitive Data.** Information/data for only internal use by authorized Reclamation employees, business partners, and customers through established "Access Controls." The unauthorized, inadvertent, or deliberate disclosure, alteration, use, or destruction of such information/data which could effect Reclamation's ability to perform agency functions, impede daily business activities, and/or effect employee productivity. Release to the public requires prior approval from a manager/system owner.

4. **Scope.** This Directive and Standard applies to IT equipment used for any of the following purposes: access by multiple users; hosting of critical/major applications; or containing restricted/sensitive information. This includes IT equipment used in energy and water operations, i.e., Supervisory Control and Data Acquisition systems.

5. **Procedures.**

A. **Access to Restricted and Sensitive Data.**

(1) Access to Reclamation restricted or sensitive data will be limited to only those individuals who have been properly cleared for access pursuant to DM Part 441 and Reclamation ITSP Directives and Standards.

(2) Restricted and sensitive data and its associated computer equipment will be housed in a secure environment, protected from unauthorized access and natural disruptions. Specific physical regulations required for sites housing IT equipment which process restricted, sensitive, or uniquely important data are indicated below.

B. **Secure Housing Structures.** IT equipment which processes restricted, sensitive, or uniquely important data will be:

(1) Located in a room, building, or office which can be closed and locked. Space will be locked during off-duty hours.

(2) Housed away from areas where serious man-made catastrophes could occur (e.g., chemical spills, near motor vehicles, etc.).

(3) Limited access and restricted from unescorted or unprotected public access.

(4) Housed in areas with no identifying signs (e.g., computer room, wiring closet, etc.).

(5) Accessed through doors which are self-closing, lockable (accessible through either magnetic cards, cypher locks, combination locks, keyed locks), and have alarm feature for the door ajar for an extended period of time. Any type of non-keyed lock should have a keyed backup.

C. **Access Restrictions.**

(1) **Access to IT Spaces.** Access to all IT spaces will be limited to authorized personnel with proper identification. This access is limited to personnel whose duties require frequent access to these facilities and will be monitored.

(2) **Computer Room Visitor Restrictions.**

(a) Computer room visitors will not have in their possession inappropriate material including weapons, cameras, recording devices, etc., and must receive authorization/clearance for entry from appropriate Reclamation staff.

(b) All visitors will be escorted by a Reclamation employee(s).

(c) Visitors will be limited to access during business hours or as appropriate scheduling requires.

(d) Visitors must sign in and out.

(e) Visitors will wear temporary badges at all times during visits.

(f) Visitors without badges will be challenged by Reclamation employees and contractors and not allowed access.

(3) **Card Key Access.** Physical access and security of Reclamation facilities will be addressed and managed pursuant to a Directive and Standard currently under development.

(4) **Open Doors.** When a door to a computer or data active/storage area must be propped open, a Reclamation employee will be present to ensure no unauthorized access takes place.

(5) **Piggy-Back Access.** Each employee must be verified through his/her card key or visitor pass before being allowed access into controlled computer rooms. No piggy-back entrance behind an authorized employee/contractor is permitted.

(6) **Intermediate Holding Area.** For active computer areas, an intermediate holding area for visitors is strongly suggested.

(7) **Terminated and Transferred Employees and Contractors.** Upon the termination or transfer of an employee or contractor, access to the computer room will be terminated by close of business on the day the employee leaves.

(8) **Validated Employees and Contractors List.** A current list will be maintained of all validated employees and contractors who have been granted access to those spaces where IT equipment and data is used and/or stored.

D. **Physical Data Storage Requirements.** Sensitive and restricted data will be stored in secured areas, as noted above, with access allowed only to those approved employees and contractors meeting the appropriate background clearances and granted access privileges pursuant to their need to know.

E. **Computer Room Design.** Computer room design will include the following considerations:

- Power requirements, e.g., proper grounding of equipment, uninterruptible power supply, filters to control spikes and surges, etc.
- Environmental controls (temperature and humidity)
- Fire safety (installation of sprinklers, etc.)
- Hazard detection devices for flooding, fire, and physical intrusions.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the ITSP in Reclamation.

B. **Directors of Reclamation Regions and Offices.** Directors of Reclamation Regions and Offices have responsibility for ensuring the security of IT systems under their authority. This responsibility may be delegated no more than one level down (Deputy or Assistant Directors).

C. **Reclamation IT Security Managers.** Reclamation IT Security Managers will coordinate with Site/Physical Security Managers to ensure adequate physical security for IT operations.

D. **Reclamation Managers.** Reclamation Managers will support the ITSP by ensuring compliance with this Directive and Standard.

7. **Related Directives and Standards.** For related and supporting Directives and Standards see the Information Resources Management (IRM) section of the Reclamation Manual.