Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Network Systems

Purpose: Establishes the standards, requirements, and procedures supporting all Reclamation networks as part of the ITSP.

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-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); The Computer Security Act of 1987 (Public Law 100-235); Fiscal Year 2001 Defense Authorization Act (Public Law 106-398) including Title X, Subtitle G, *Government Information Security Reform*; OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); Special Publication 800-10, *Keeping Your Site Comfortably Secured: An Introduction to Internet Firewalls*, National Institute of Standards and Technology (NIST); Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*; and DM Part 377, *Telecommunications*.

Contact: Information Resources Services Office, D-7100

1. **Introduction.** This Directive and Standard establishes a network security architecture under the ITSP which provides management direction, procedures, and requirements to ensure the appropriate protection of Reclamation information created, acquired, controlled, displayed, transmitted, or received by Reclamation networks. All exceptions to this Directive and Standard must be approved by the Chief Information Officer (CIO) or his/her delegated representative.

2. **Goal.** The goal of this Directive and Standard is to establish management direction, procedures, and requirements to ensure the appropriate protection of Reclamation information handled by computer networks.

3. **Definitions.**

   A. **Network Perimeter.** The boundary between any Reclamation IT system and any non-Reclamation IT system.

   B. **Network Devices.** Any device which is traversed by data traveling from one device to another (not including the source/destination end points). Also included is any equipment which controls or monitors these devices or the data transmitted by them.

C. **Security Mechanisms.** Hardware and/or software products used to secure Reclamation IT systems and networks [e.g., firewalls, screening routers, intrusion detection systems (IDS), virtual private networks (VPN), anti-virus software, proxy servers, and authentication servers].

D. **Third Parties.** Authorized non-Reclamation users or organizations which integrate with Reclamation network services in order to perform a function in support of their mission. This mission may or may not be coordinated with goals and objectives of Reclamation.

E. **Remote Access.** Temporary authorized access established from any external system or computer to a Reclamation IT system or network.

F. **Security Zones.** Logical design areas, both inside and outside a network security perimeter, with predetermined levels of protection and security protocols, e.g., demilitarized zones (DMZ).

4. **Scope.** This Directive and Standard applies to all Reclamation employees, contractors, consultants, and volunteers, including those affiliated with third parties who access Reclamation networks. It applies to all IT and telecommunication systems owned by and/or administered by Reclamation, including specialized systems [e.g., Supervisory Control and Data Acquisition Systems (SCADA), Hydromet, Geographic Information Systems (GIS)].

5. **Procedures.**

A. **Establishing Network Connections.**

(1) Employees may not install telecommunication services or circuits with any communication carrier except as defined in DM Part 377 and Reclamation Wide Area Network (WAN) and Telecommunications Standard Operating Procedures.

(2) Employees may not install new local area networks (LAN) or extend existing LANs that cross the perimeter without prior approval from their Regional Director or Office Director (e.g., Director, Technical Services Center; Director, Management Services Office) or his/her delegated representative. Employees must also adhere to Reclamation WAN and Telecommunication Standard Operating Procedures and other Directives and Standards for Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., SCADA, GIS, Hydromet). Such installations will be documented consistent with guidance in the ITSP Configuration Management Directive and Standard.

(3) Physical connections between two or more Reclamation computer systems that cross security zones must adhere to Reclamation WAN and Telecommunication Standard Operating Procedures and other Directives and Standards for Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., SCADA, GIS, Hydromet).

B. **Configuration Management of Network Devices.** Changes to Reclamation network devices, including but not limited to: loading new software; changing network addresses; reconfiguring routers, firewalls, switches, or hubs; and adding telecommunication lines, are strictly limited to those processes authorized in Reclamation WAN and Telecommunication Standard Operating Procedures and other Directives and Standards for Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (SCADA,GIS, Hydromet).

C. **Security Mechanisms.**

(1) All connections between networks of different security zones must traverse an approved Reclamation-managed security mechanism. All data crossing these security mechanisms will be checked for computer viruses and other malicious code which may compromise the security of Reclamation IT infrastructure. Data checking does not necessarily mean dropping or interrupting data flow, especially on specialized systems.

(2) All Reclamation firewalls are managed according to NIST Special Publication 800-10, *Keeping Your Site Comfortably Secured: An Introduction to Internet Firewalls*. Each firewall will have a designated primary and secondary administrator.

D. **Third-Party Access.** As a prerequisite for connection, every third party seeking access to Reclamation IT systems or networks must agree, via a formal Interagency Agreement or Memorandum of Understanding, to comply with Reclamation ITSP Directives and Standards.

E. **Remote Access.** All remote access connections will use a Reclamation-approved access control point as defined in the Remote and Third-Party Access Directives and Standards.

F. **System Security.**

(1) IT systems connected to Reclamation networks must comply with all relevant Reclamation ITSP Directives and Standards.

(2) All network monitoring devices must be used in accordance with Reclamation WAN and Telecommunication Standard Operating Procedures and other

Directives and Standards for Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., SCADA, GIS, Hydromet).

G. **Network Security Information.**

(1) Information regarding security measures for Reclamation computer and communication systems is restricted and should be treated in accordance with the Information/Data Security Directives and Standards.

(2) The internal system addresses, configurations, and related system design information for Reclamation networked IT systems and network devices will be restricted to authorized personnel defined in the ITSP Configuration Management of Security Mechanisms Directives and Standards.

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 the security of the 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 (ITSM).** ITSMs support Reclamation Directors/Managers in the formation and coordination of processes to ensure the network security architecture is adequate, appropriate, and supports Reclamation-wide IT security Policy and Directives and Standards. The ITSMs facilitate compliance with security architecture restrictions and requirements. The Bureau ITSM (BITSM) coordinates with the ITSMs and acts as liaison to the Manager, Information Resources Services or the CIO as appropriate.

D. **Reclamation Employees.** Reclamation employees are responsible for compliance with ITSP Directives and Standards and those who willingly and deliberately violate them will be subject to disciplinary action identified in Public Law 99-474.

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