Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Configuration Management of Security Mechanisms

Purpose: Establishes the processes, goals, and objectives for managing and maintaining security mechanisms protecting Reclamation IT systems and networks and to define the authority, responsibility, and accountability for configuration management.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); The Computer Security Act of 1987 (Public Law 100-235); Fiscal Year 2001 Defense Authorization Act (Public Law 106-398), Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); OMB Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); Department of the Interior Departmental Manual Part 375, Chapter 19, *Information Technology Security*.

Contact: Information Resources Services, D-7100

1. **Introduction.** This Directive and Standard establishes standards and procedures for controlling, operating, and maintaining approved Reclamation-managed security mechanisms consistently and cost effectively across Reclamation.

2. **Goals.** The goals for configuration management of security mechanisms are:

   A. Maintain the continuity of Reclamation operations by preventing or minimizing the adverse impact of changes to IT security mechanisms.

   B. Establish the requirement for change request process.

   C. Protect security mechanism configurations (clearly defined, non-ambiguous rule sets, lists, drawings, etc.) from unmanaged changes or version compatibility problems.

   D. Maintain thorough and complete configuration management documentation including records of changes, restorable configurations, and documentation of the reason for changes.

3. **Definitions.**

   A. **Reclamation-Managed Security Mechanisms (Security Mechanisms).** Hardware and/or software products used to secure Reclamation's 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].

   B. **Configuration Management.** Umbrella activity developed to (1) identify change, (2) test and implement the change, (3) enforce change procedures, (4) report the change to others, and (5) record the change for historical reference (e.g., for restoration of a working configuration).

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

   D. **Restorable Configuration.** Configurations that can be restored from backup tapes, system logs, and other documentation.

4. **Scope.** Applies to security mechanisms protecting Reclamation-owned, -operated, and -maintained IT systems, including specialized systems [e.g., Supervisory Control and Data Acquisition Systems (SCADA), Hydromet, Geiographic Information Systems (GIS), Dam Safety].

5. **Procedures.**

   A. **Assignment of Responsibilities**. Responsible personnel will be identified and assignments made to ensure Reclamation-wide coordination and effective implementation of configuration management procedures. See paragraph 6C (Administrators).

   B. **Compatibility of Security Mechanisms.** Security mechanisms must be compatible network-wide to ensure the integrity of the network perimeter. Administrators, working with Regional Information Technology Security Manager (ITSM) and Bureau ITSMs (BITSM), will document and maintain a security mechanism inventory database including license information, hardware and software descriptions and standards, software versions and patches, configurations, and maintenance contracts information.

   C. **Security Mechanism Updates.** Administrators evaluate the performance of security mechanisms in the inventory database and define technology upgrades to meet mission requirements. These decisions are documented in a change request process as described in the IT Security Configuration Management Procedures. The change request process also defines who has the authority to make changes, the process required for approval, and the process of coordination with the appropriate support services. Additions and changes to existing security mechanisms are tested at approved test labs before installation.

D. **Coordination.** Administrators coordinate the deployment and operation of security mechanisms including distribution, system documentation, training, testing, and integration with appropriate support services.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the ITSP in Reclamation. 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). The Manager, Information Resources Services has overall responsibility for managing the security architecture of Reclamation's IT infrastructure.

B. **Reclamation's IT Security Managers (ITSM).** ITSMs support the formation and coordination of processes to ensure all security mechanisms are adequate, appropriate, and support the Reclamation-wide IT security policy and Directives and Standards. ITSMs ensure compliance with IT Security Configuration Management Procedures. The BITSM coordinates the activities of the ITSMs and acts as liaison to the Manager, Information Resources Services, or the CIO as appropriate. ITSMs and Administrators will coordinate with IT technical staff to ensure effective implementation of configuration management practices.

C. **Administrators.** Network Security Administrators, Remote Access Administrators, Firewall Administrators, IDS Administrators, Extranet System Administrators, and Client Administrators (e.g., help desk) are responsible for:

(1) coordinating the deployment and operation of security mechanisms;

(2) monitoring the performance of security mechanisms;

(3) ensuring consistency between the configurations of the security mechanisms they are responsible for and the Reclamation-wide security mechanism database; and

(4) participating in the change process as defined in the IT Security Configuration Management Procedures.

7. **Related Directives and Standards.** Related Directives and Standards are found in the Information Resources Management (IRM) section of the Reclamation Manual.