Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): IT System Security Accreditation

Purpose: Describes the process for IT system security accreditation.

Authority: The Privacy Act of 1974 (5 U.S.C. § 522a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); OMB Circular 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*; *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (January 2000); Federal Information Processing Standard (FIPS) Publication 102, *Guideline for Computer Security Certification and Accreditation*; Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, National Institute of Standards and Technology (NIST); and 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 procedures for IT system security accreditation and reaccreditation. It identifies the steps and describes the roles within Reclamation required to establish adequate IT security controls.

2. **Goals.**

   A. To incorporate IT system security certification and accreditation into the business practices of Reclamation and to ensure that major applications and general support systems are authorized to operate and are reauthorized every 3 years or in the event significant changes are made.

   B. To ensure IT security controls are in place and adequate for the level of data sensitivity.

   C. To ensure IT security for the accredited system and the system(s) with which the system may interface.

3. **Definitions.**

A. **Accreditation.** The authorization granted to an IT system to operate made on the basis of a certification by designated accrediting officials that the design and implementation of the system meet requirements for achieving adequate data security. Accreditation follows assessment and mitigation of risks and vulnerabilities and completion of an IT system security plan.

B. **Accrediting Official.** Directors of Reclamation offices and regions who have the authority to accept a system's security safeguards and issue an accreditation statement. The accrediting official must have authority to allocate resources to achieve acceptable security and to remedy security deficiencies, including authorization to suspend the operation of the system in the event of severe system compromise.

C. **Certification.** The technical evaluation made in support of the accreditation process that establishes the extent to which an IT system meets a specified set of security requirements.

D. **General Support System (GSS).** An interconnected set of IT resources under the same management control that share common functionality. A GSS normally includes hardware, software, information, applications, communications, facilities, and people and provides support for a variety of users and applications. GSSs provide security for the applications that execute in their environment.

E. **IT System Security Plan.** A plan addressing the adequate security of a major application or general support system. Accreditable plans must be consistent with the guidance provided in NIST Special Publication 800-18.

F. **Major Application.** An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information related to the application. In Reclamation, major applications are those which are key to achieving Reclamation performance goals.

G. **Rules.** The part of the IT system security plan which clearly delineates the responsibilities of and expectations for all individuals with access to an IT system.

H. **Significant Changes.** Any major change or new finding that calls into question an accreditation decision, such as major changes in requirements, occurrence of a significant violation, or audit findings.

4. **Scope.** This Directive and Standard applies to all IT and telecommunications systems owned and/or administered by Reclamation, including specialized systems (e.g., Supervisory Control and Data Acquisition Systems, Hydromet, Geographic Information Systems, etc.).

5. **Procedures.**

A. **Accreditation Steps.** Applications designated as "Major Applications" and systems designated as "General Support Systems" require IT system security accreditation to be accomplished as part of system life cycle planning and, to the greatest extent possible, as part of an overall certification and accreditation effort addressing all types of authorization and management control review requirements. For those systems identified as Major Applications and General Support Systems, the following steps apply:

(1) **Asset Valuation.** An evaluation is performed to determine an IT system's criticality.

(2) **Assign Risk.** An assessment is performed to identify potential threats and define a system's acceptable level of risk.

(3) **Develop Rules.** Written rules concerning the security and use of a system and define expected behaviors for all individuals with access to the system. The security required by the rules can be only as stringent as necessary to provide adequate security for the system.

(4) **Assign Responsibility.** Security for each general support system is assigned to an individual knowledgeable in the information technology used in the system and in providing security for such technology. Security responsibility for each major application is assigned to a management official knowledgeable in the nature of the information and processes supported by the application. Risks, rules, and responsibilities are included in the IT system security plan.

(5) **Certify.** Certification consists of a technical evaluation of a system to determine how well it meets its security requirements. Certification steps are described in FIPS Publication 102, *Guideline for Computer Security Certification and Accreditation.*

(6) **Accredit.** Accrediting officials use the certification report to evaluate a system's security effectiveness. They then decide on the applicability of the safeguards, ensure that corrective actions are implemented, and issue the accreditation statement that authorizes system operation. The accreditation statement is part of the certification report. See FIPS Publication 102, *Guideline for Computer Security Certification and Accreditation.*

(7) **Monitor Performance.** Accrediting officials institute performance measures and management processes that monitor actual performance of security safeguards and

compare actual performance to expected results. Performance measuring tools include safeguard evaluations; validation, verification, and testing (VV&T); and security audits.

B. **Recertification and Reaccreditation.** General support systems and major applications are reaccredited every 3 years or in the event significant changes are made. Recertification requires the review and update of system specific security plans for accuracy and effectiveness. As needed, corrective actions are identified and implemented, and the system is then reauthorized for operation. Refer to FIPS Publication 102, *Guideline for Computer Security Certification and Accreditation* for specific guidance in reaccreditation.

6. **Responsibilities.**

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

B. **Directors of Reclamation Regions and Offices (Accrediting Officials).** Directors of Reclamation Regions and Offices have responsibility for accrediting and ensuring the security of IT systems under their authority. This responsibility may be delegated no more than one level down (Deputy or Assistant Directors). Accrediting officials are responsible for authorizing or re-authorizing, in writing, the use of IT system(s).

C. **Reclamation Regional IT Security Managers (ITSMs).** ITSMs develop and coordinate processes to support accrediting officials in establishing and verifying system accreditation and ensuring that these processes are adequate, appropriate, and support Reclamation-wide IT security policy.

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