Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Computer Application Development, Acquisition, and Maintenance

Purpose: Describes Reclamation's standards for assurance of IT security in computer applications used within Reclamation.

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) including Title X, Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); 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); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); and Department of the Interior Departmental Manual Part 375, Chapter 19, *Information Technology Security*.

Contact: Chief Information Officer, D-2200

1. **Introduction.** This Directive and Standard describes security requirements for the development, acquisition, and maintenance of computer applications, and establishes requirements for the development and maintenance of security controls.

2. **Goal.** To protect Reclamation from threats [as defined in Reclamation Manual (RM), *Reclamation Information Technology Security Program*, IRM P01] by including security standards in application design and/or development practices, and also to protect Reclamation's applications from threats through proper maintenance or operation procedures.

3. **Definitions.**

   A. **Live Data.** Information currently being used by a production system or application. This includes real-time data in control systems and remote sensing applications, as well as production databases.

   B. **Life-Cycle Planning.** A systematic approach that provides a structured process for planning and administering IT from concept to disposal. National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security*, defines and provides details on the following five phases:

(1) **Initiation Phase.** During this phase, the need for a system is expressed and the purpose is documented.

(2) **Development/Acquisition.** During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

(3) **Implementation.** After initial system testing, the system is installed or deployed.

(4) **Operation/Maintenance.** During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.

(5) **Disposal.** Involves the disposition of information/data, hardware, and software, once the decision has been made to decommission the system.

4. **Scope.** This Directive and Standard applies to:

A. All Reclamation-owned, -developed, or -procured IT systems, including software, hardware, telecommunications, or combinations thereof. Systems procured for others under memorandums or agreement or understanding are also included.

B. Reclamation IT systems in the proposal, design, or development processes.

C. All Reclamation employees and contractors having responsibility for the proposal, design, development, and/or procurement of IT systems for use within or for Reclamation.

5. **Procedures.**

A. **IT Security References for Applications.** All application planners, developers, and maintenance technicians will apply the principles found in the NIST publications 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*; 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; and 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

B. **Accreditation.** All major applications (as defined in RM, *IT System Security Accreditation*, IRM 08-07) must be accredited in accordance with that standard. New applications must have an Interim Authority to Operate (IATO) in place or be accredited prior to operation. Documentation for accreditation includes a risk

assessment, application-specific security and contingency plans, and a test plan and report. Re-accreditation must occur every 3 years or whenever a significant change to the application or host system occurs.

C. **Coordination.** Sensitive data in the application can affect the management of related General Support Systems and applications. IT security controls required for the application should be coordinated with the appropriate IT Security Manager(s). In addition, IT System Security Plans for the related general support systems and applications should be cross referenced to ensure cross-platform, system, or application security relationships are well-understood and appropriately considered.

D. **Application Testing.** All new or significantly modified applications will undergo extensive testing to ensure reliability of the system, and to ensure all needed security controls are operational. Testing should be conducted in accordance with the Application Security Plan or procurement specifications and will ensure/complete the following:

(1) All technical and physical safeguards are in effect and performing as specified.

(2) No live, restricted, or sensitive data will be used during testing unless interim approval to operate has been granted. Reference the NIST Special Publication 800-37, *Guidelines for the Certification and Accreditation of Federal Information Technology Systems*, for further details. Parallel source data where available, may be employed to test the security and functional performance of real-time systems. Where employed, parallel source data feeding the test system must not interfere with the performance of the production system in any way and must not be reintroduced into any production system after being processed in the test system.

(3) Any testing of systems containing live data will be very closely monitored to ensure system continuity of operations, conformance to legal obligations, and life and property safety. The test plan will ensure that appropriate, tested, backup capabilities are in place in the event that an accident/incident does occur.

E. **Life Cycle Security Design.** Security, like other aspects of an IT system, is best managed if planned for throughout the IT system life cycle. Security will be a fundamental aspect during all five phases of an application's life cycle. The following procedures will occur during the delineated phases:

(1) **Initiation.** Assess the possible criticality/sensitivity of the application and related data, and data retention and disposition requirements. Based on these factors, define the baseline security requirements of the application.

(2) **Development/Acquisition.** Design application security controls to meet the requirements identified in the Initiation phase. Where requirements are identified and specified for procurement purposes, establish key evaluation criteria that can be used for security control validation.

(3) **Implementation.** Install and turn on IT security controls prior to any final security testing and before IATO or certification and accreditation.

(4) **Operation/Maintenance.** Maintain and administer system configuration and security (e.g., system documentation, operational assurance, audits, and monitoring). Reaccredit as required.

(5) **Disposal.** Disposal of the application and disposition of related data will comply with the RM, *IT Asset Disposal*, IRM 08-13.

F. **Application Access Controls.** Access controls will be in accordance with RM, *Computer Protections, Anti-Virus, Access Control, and Passwords*, IRM 08-12. Data access permission will be commensurate with the information sensitivity as defined in RM, *Information/Data Security*, IRM 08-11.

G. **Documentation Storage.** Security plans, design specifications, source code, memoranda of understanding, and contingency plans are considered vital records and backup copies will be stored in accordance with RM, *Continuity of Operations*, FAC 05-01.

H. **Configuration Management.** Application configuration management is a key component of application security. The effective implementation of configuration management for an application's components (code, hardware, documentation, training, support, etc.) is required.

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).** Accrediting Officials have responsibility for accrediting and ensuring the security of the 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 reauthorizing, in writing, the use of IT systems(s).

C. **Application Owners.** Application Owners are responsible for managing the security, configuration, operation, maintenance, and proper use of their applications. They are also responsible for coordinating with the Records Officers to determine the retention and disposition requirements for the application's data. Each application owner will identify a system security manager responsible for security throughout the life cycle.

D. **Information Technology Security Manager (ITSM).** The appropriate ITSM will assist computer application developers and designers in identifying security requirements to ensure compliance with the ITSP. The ITSM will assist the business owner and application developer with completing activities associated with the accreditation of the application.

E. **IT Application Developers/Maintenance Technicians.** Computer analysts, engineers, and others who may design, develop, or specify requirements for computer applications and/or systems are required to adhere to this Directive and Standard and to coordinate with local IT security staff.

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