Reclamation Manual

Directives and Standards

Subject: Bureau of Reclamation Information Technology Security Program: Configuration Management.

Purpose: Establishes the general requirements for configuration management of Reclamation general support systems and major applications.

Authority: Computer Security Act of 1987 (Public Law 100-235);

Federal Information Security Management Act of 2002 (Public Law 107-347);

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);

National Institute of Standards and Technology Special Publication 800-12, An Introduction to Computer Security;

National Institute of Standards and Technology Special Publication 800-14, Generally Accepted Principles and

Practices for Securing Information Technology Systems; and
Department of the Interior Departmental Manual Part 375, Chapter 19, Information Technology Security Program.

Contact: Chief Information Officer, D-2200

1. **Scope.** This directives and standards (D&S) applies to all general support systems (GSS) and major applications (MA) owned, operated, or maintained by Reclamation.

2. **Introduction.** This D&S establishes requirements for identifying, controlling, accounting for, and auditing all changes affecting Reclamation GSS or MA throughout their life cycle. Configuration management begins when a system or application is being designed or developed, continues during operations and maintenance, and ends when the system or application has been decommissioned or destroyed at the end of its useful life.

3. **Responsibilities.**

   A. **Chief Information Officer (CIO).** The CIO has overall responsibility for configuration management of Information Technology (IT) Systems in Reclamation.

   B. **Reclamation's IT Security Managers (ITSM).** ITSMs participate in the configuration management process to ensure that security is not degraded, but only enhanced (or maintained at the same level) as a result of changes. The Reclamation ITSM coordinates the activities of all other ITSMs and acts as liaison to the CIO. ITSMs and administrators will coordinate with all IT technical staff to ensure effective implementation of configuration management practices.

C. **Executive System Owners.** Directors of Reclamation regions and offices, serving as Executive System Owners (ESOs), are responsible for the configuration management of GSS's and MA's under their authority. This responsibility may be delegated no more than one level down (deputy or assistant directors). They are required to establish Configuration Control Boards (CCB) to manage all the components of their systems. The ESO must fully understand the configuration and changes being made, and must approve all changes. (The authority to approve changes can be delegated to the chairperson of the CCB.)

D. **IT Portfolio System Project Managers.** IT Portfolio System Project Managers are responsible to identify configuration items and establish configuration management procedures.

E. **System Security Managers.** System Security Managers are the principal technical advisors to the ESOs and the IT Portfolio System Project Managers for all security-related issues, and are key members of the CCB.

F. **Reclamation IT Technical Teams.** For those systems which include platforms supported by Reclamation IT Technical Teams, these teams are responsible to provide consulting, coordination, standards, procedures, and testing. IT Technical Teams will recommend changes to the CCB, act as liaison to the CCB, and coordinate with IT technical staff to ensure effective implementation of configuration management practices.

G. **Configuration Control Board.** CCBs shall be established to review, evaluate, and approve (or disapprove) proposed changes to GSS or MA.

H. **General Responsibilities.** All Reclamation personnel and contractors actively involved in making changes (additions, deletions, or modifications) to GSS or MA during any phase of the life cycle are required to comply with configuration management requirements. This group of responsible individuals includes (but is not limited to) program managers, system engineers, quality assurance specialists, integrators and testers, installers, programmers, system and network administrators, hardware and software maintenance personnel, etc.

4. **Definitions.**

A. **Configuration Control.** The process of controlling modifications to a system's design, hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation.

B. **Configuration Control Board.** An established committee that is the final authority on all proposed changes to systems or applications.

C. **Configuration Identification.** Identifying system configuration throughout the life cycle.

D. **Configuration Item.** The smallest component of hardware, software, firmware, documentation, or any of its discrete portions, which is tracked by the configuration management. These items also include components of networks or communications systems.

E. **Configuration Management.** The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the life cycle of the system.

F. **Configuration Management Plan (CMP).** A document describing how configuration management will be implemented to achieve the four basic goals of identification, control, accounting, and auditing. It identifies the configuration items associated with the GSS or MA, and identifies specific roles and responsibilities.

G. **General Support Systems and Major Applications.** These definitions appear in Appendix III to OMB Circular No. A-130, Paragraphs A2c and A2d.

H. **System and Network Administrators.** The managers and technicians who configure and operate computer systems and networks. They are responsible to implement security safeguards, and to be familiar with security technology related to their systems. They also need to ensure the continuity of their services to meet the needs of functional managers, as well as analyzing threats and vulnerabilities affecting their systems (and probabilities of associated security risks)

5. **Goals.** The overall goal of configuration management is to maintain control of systems or applications throughout their life cycle, ensuring that all additions, deletions, or changes occur in an identifiable and controlled environment, and that such changes do not adversely affect any desired properties or functions. In particular, configuration management helps to

ensure that modifications maintain or enhance information protection, without degrading security. Specific goals include:

A. **Configuration Identification.** The goal is to identify the configuration of a system at discrete points in time for the purpose of systematically controlling changes to the configuration and maintaining the integrity and traceability of this configuration throughout the system life cycle. An important part of this goal is to identify "configuration items," which are uniquely identifiable subsets of the system configuration representing the smallest portion of the system to be subject to independent configuration management change control procedures.

B. **Configuration Control.** The goal is to systematically test, evaluate, coordinate, and approve or disapprove proposed changes to the design and construction of any configuration item whose configuration has been formally approved. An important part of this goal is to establish formal mechanisms for evaluating, coordinating, and approving (or disapproving) changes. This is accomplished by a qualified team of knowledgeable professionals of the CCB.

C. **Configuration Status Accounting.** The goal is to record and report all information considered "significant" to the configuration management process. "Significant" items are identified in the CMP for the GSS or MA. The records and reports produced through configuration status accounting should include the original designs, historical changes, the status of change requests and their implementation, and the current configuration list.

D. **Configuration Audit.** The primary goal is to ensure only authorized additions, deletions, and modifications are made. The secondary goal is to ensure that information security has not been compromised or degraded by the changes. System and Network Administrators are responsible for periodic (at least annual) audits, and will report discrepancies to the CCB.

6. **Procedures.** The following procedures will be followed to establish and maintain compliance with this D&S:

A. **Responsible Agents.**

(1) For each GSS or MA, the ESO has overall management responsibility for configuration management, and is required to establish a CCB to manage all the components of that system. The ESO must fully understand the configuration and changes being made, and must approve all changes. (The authority to approve changes can be delegated to the chairperson of the CCB). In some cases,

ESOs will be responsible for more than one GSS or MA, or individual organizations may be responsible for pre-defined parts of a GSS or MA.

(2) The IT Portfolio System Project Manager is responsible to identify configuration items and establish configuration management procedures.

(3) The System Security Manager is the principal technical advisor to the ESO and the IT Portfolio System Project Manager for all security-related issues, and is a key member of the CCB.

(4) For those systems which include platforms supported by Reclamation technical teams, the IT Technical Teams are responsible to provide consulting, coordination, standards, procedures, and testing. IT Technical Teams will recommend changes to the CCB, act as liaison to the CCB, and coordinate with IT technical staff to ensure effective implementation of configuration management practices.

B. **Configuration Control Board.** For each system included in the current Reclamation IT portfolio, select a chairperson and the group of knowledgeable professionals who will review, evaluate, and approve (or disapprove) changes. As circumstances require, depending on the nature of changes being considered, include other key individuals from physical security, facilities, quality assurance, etc. as members of the CCB. It may be advisable to establish sub-groups to address specific issues or areas of concern.

(1) The CCB will meet on an as-required basis to approve or disapprove changes, but it is expected that members will communicate with each other regularly by e-mail, telephone, and similar means during the review and evaluation process. Maintain copies of meeting minutes for at least 2 years, since these minutes are formal documentation of approved (or disapproved) changes.

7. As stated above, the ESO can give the chairperson of the CCB authority to approve or disapprove changes However, if proposed changes involve expenditure of funds, the CCB chairperson must be a person who is authorized to expend funds.

A. **Configuration Management Plan.** Prepare a CMP for each system included in the current Reclamation IT portfolio. A single CMP can address multiple systems or applications. The CMP will describe how configuration management is being (or will be) accomplished for the GSS or MA, and it will identify the configuration items for each system or application. The CMP will be approved and signed by the chairperson of the CCB. The CMP is a living document, frequently updated, which includes at least the following items:

(1) CCB members, probably listed by title or position rather than by name.

(2) Roles and responsibilities of CCB members.

(3) System or application description and list of configuration items.

(4) Any tools available to assist in the configuration management process.

(5) Normal procedures for configuration identification, control, accounting, and audit.

(6) Emergency procedures to be followed when a change must be implemented immediately.

(7) How impacts on related systems will be addressed.

8. **Related Directives and Standards.** Related D&S are located in the Information Resources Management section of the Reclamation Manual at www.usbr.gov/recman .