Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Audit and Systems Logging

Purpose: Describes Reclamation's IT systems audit and logging standards, requirements, and procedures.

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 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 (DM) Part 375, Chapter 19, *Information Technology Security;* and Special Publication 800-10, *Keeping Your Site Comfortably Secured: An Introduction to Internet Firewalls*, National Institute of Standards and Technology (NIST).

Contact: Information Resources Services, D-7100

1. **Introduction.** This Directive and Standard establishes system logging requirements and ITSP audit processes.

2. **Goal.** The goal of this Directive and Standard is to ensure that the ITSP is correctly implemented throughout Reclamation and that system/audit logs provide the necessary information to log and track IT security incidents.

3. **Definitions.**

   A. **IT Audit.** The process of verifying and documenting IT security practices for a system, device, network, or location.

   B. **System/Audit Log.** A record of system activities. In conjunction with appropriate tools and procedures, system/audit logs can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.

4. **Scope.** This Directive and Standard applies to all Reclamation employees and contractors involved in the management of shared IT systems, including system administrators (SAs) and IT security personnel. IT systems include:

A. Reclamation-owned, -operated, and -maintained IT systems, including specialized systems [e.g., Supervisory Control and Data Acquisition Systems (SCADA), Hydromet, Geographic Information Systems (GIS), Dam Safety].

B. All Reclamation-owned IT systems operated and/or maintained by contract or temporary personnel.

C. All Reclamation-owned IT systems operated and/or maintained by organizations or personnel other than Reclamation.

5. **Procedures.**

A. **IT Security Audits.** IT security audits will be performed at each Reclamation site periodically to ensure compliance with IT security policies and Directives and Standards. Each audit will:

(1) Follow prepared and approved checklist(s) of items requiring review. Checklists are succinct lists of items referenced in Reclamation Directives and Standards and DM IT Security requirements, including the IT System Security Plans (ITSSP), accreditation documentation, training, IT Continuity of Operations Plans, etc.

(2) Complete on-site reviews within a reasonable period of time, usually less than 2 working days, to minimize disruptions of operational staff.

(3) Report findings to the Bureau Information Technology Security Manager (BITSM) and Office/Regional Director or his/her delegate, with certification signatures of audit completion by the local office and IT managers.

(4) Be performed at a minimum of every 3 years, unless a significant non-compliance is discovered, which will require a follow-up audit within 6 months to ensure the business practice has been corrected.

B. **IT Security Logging Requirements.** IT systems with logging capability will activate logging and use supporting software to read and interpret logs. Integrity and confidentiality of system logs will be protected from unauthorized access. SAs will monitor system logs and report security incidents to their Regional Information Technology Security Manager (ITSM) as instructed in the IT Security Incident Handling Capability (Procedures). In addition, logs from the following software will be monitored:

(1) Intrusion detection software as detailed in the Reclamation ITSP Intrusion Detection Systems Directive and Standard;

(2) Firewall security mechanisms; and

(3) Anti-virus, password maintenance, and access control software, as described in the Reclamation ITSP Computer Protection, Anti-Virus, Access Control and Passwords Directive and Standard.

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. **Bureau Information Technology Security Manager (BITSM)/Regional Information Technology Security Manager (ITSM).** The Regional ITSM will coordinate IT security audits and report results to appropriate Office/Regional Director and the BITSM. The BITSM will approve the checklist prior to each audit.

D. **IT Security Auditor.** Reclamation employees and contractors with rotating assignments to perform IT security auditing in locations other than their permanent duty location. Assignments are temporary and considered collateral duties. Assignments will be made outside of permanent duty regions whenever feasible. Typically IT auditors will be IT technical experts, security managers, or SAs (e.g., SCADA administrators) with substantial IT/network expertise.

E. **System(s) Administrator**. SAs are responsible for activating and monitoring system logs and participating in site IT security audits.

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