Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Program: IT Intrusion Detection Systems (IDS)

Purpose: Establishes the IDS standards, requirements, and procedures supporting Reclamation's IT Security Program (ITSP).

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 (January 2000); 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 guidance for how and where IDS should be applied on IT systems exposed to the Internet and other threats, and defines the minimum requirements and standards for IDS operation. The detection of unauthorized access to Reclamation systems is essential for the protection of Reclamation IT assets.

2. **Goals.**

   A. Reduce the risk of undetected intrusion to Reclamation's IT systems and thereby minimize the possibility of damage to those systems and their data.

   B. Gather information about the types of data/information corrupted, deleted, and/or collected from compromised systems, for the purposes of limiting damage and alerting appropriate security/protective personnel.

   C. Provide documentation (evidence) of intrusions necessary to support prosecution of IT intruders or other IT system attackers, and to report and coordinate within Reclamation and IT security monitoring organizations (e.g., Federal Computer Incident Response Capability and the "InfraGard" program administered by the Federal Bureau of Investigation).

3. **Definitions.**

   A. **Intrusion Detection Tools/Systems.** Products and methodologies used to detect intrusions into a company's or agency's IT systems.

   B. **Multi-Layered Intrusion Protection.** A security strategy designed to provide a number of security layers. Each layer has a different aspect of protection and assurance.

   C. **Host-Based IDS.** An IDS employing software on a particular IT system (e.g., a computer node) for monitoring intrusion attempts on that system. The software uses log files and/or system auditing agents as sources of data.

   D. **Network-Based IDS.** An IDS employing network-based monitors which examine the traffic on a network segment at the data source.

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

   F. **Security Zone.** Logical design areas, both inside and outside a network security perimeter, with predetermined levels of protection and security protocols, e.g., demilitarized zones (DMZ).

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

   A. All Reclamation-owned, -operated, and -maintained IT systems which may interface with external networks, including specialized systems (e.g., Supervisory Control and Data Acquisition Systems, Hydromet, Geographic Information Systems, Dam Safety).

   B. All Reclamation-owned IT systems which may interface with external networks and are operated by and/or maintained by contract or temporary personnel.

   C. All Reclamation-owned IT systems which may interface with external networks and are operated by and/or maintained by organizations or personnel other than Reclamation.

   D. All network paths crossing Reclamation's network perimeter.

5. **Procedures.**

   A. **IDS in the DMZs.** Continuous operation of IDS is required for networks and hosts in the DMZs. IDS will be managed and operated by personnel identified by the Manager,

Information Resources Services and Regional Information Resources Management (IRM) Coordinators.

B. **IDS on Internal Network and Hosts.** IDS installations are required for internal networks and hosts when recommended by IT security risk assessments.

C. **IDS Data.** IDS will monitor all traffic crossing the Reclamation network perimeter for intrusion detection purposes. Reclamation host-based IDS software will use system log files and/or system auditing agents as source data and will supplement the network-based IDS software as a second level of the multi-layered intrusion protection mechanism. Processes will be developed by IDS administrators to collect information used for intrusion detection documentation and auditing purposes.

D. **Reporting Intrusions.** In accordance with Reclamation IT Incident Handling Procedures, IDS will provide information pertinent to the resolution and/or possible litigation of intrusions on Reclamation's systems

E. **IDS Configuration Management and Testing.** To minimize the impact of IDS on regular network traffic, the IDS will be tested prior to installation and monitored during operation. Changes to the IDS must comply with the Configuration Management Directive and Standard.

F. **Retention of Logs.** See Audits and System Logging Directive and Standard for logging, audit, and retention requirements for IDS.

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. **Reclamation's IT Security Managers (ITSMs).** ITSMs support Reclamation Director/Managers in the formation and coordination of processes to ensure the IDSs are adequate, appropriate, and support Reclamation-wide IT security policy and Directives and Standards. The ITSMs facilitate compliance with security architecture restrictions and requirements. The Bureau ITSM coordinates with the ITSMs and acts as liaison to the Manager, Information Resources Services or the CIO, as appropriate.

D. **Assigned Technical Personnel.** Assigned technical personnel have the responsibility to operate, manage, and monitor each IDS, report incidences through the Reclamation IT Security Incident Handling Procedures, and provide related technical support.

7. **Related Directives and Standards.** Related Directives and Standards are found in the IRM section of the Reclamation Manual.