Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program: Remote and Third-Party Access

Purpose: Establishes requirements for remote and third-party access connections to Reclamation's networked IT systems.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); Office of Management and Budget (OMB) Circular No. 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*; OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); and Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*.

Contact: Information Resources Services, D-7100

1. **Introduction.** This Directive and Standard describes the security requirements for remote and third-party IT systems connecting to Reclamation's internal IT systems or networks in order to minimize vulnerabilities associated with these types of accesses.

2. **Goals.** Remote network access will be consolidated and standardized to reduce risk while still enabling mission accomplishment. Connections with external partners will be secure.

3. **Definitions.**

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

   B. **Remote Access.** Temporary authorized access using a routed protocol to Reclamation's network established from outside the network perimeter.

   C. **Routed Protocol.** Protocol that can be routed by a router. A router must be able to interpret the logical internetwork established by that routed protocol, i.e., a protocol able to find a path to a destination host through a network.

   D. **Third-Party.** An authorized non-Reclamation user or organization using long-term, integrated Reclamation network services and/or information in order to perform a

function in support of their mission. This mission may or may not be coordinated with the goals and objectives of Reclamation.

4. **Scope.** This Directive and Standard applies to the remote and third-party access to:

   A. All 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. **Access Approval.** All equipment used for the access privileges defined below must adhere to paragraphs 5B and 5C below.

      (1) **Remote Access.** Access to Reclamation internal networks from remote locations will be approved in advance by the appropriate Reclamation Director or his/her designee(s). Remote access may be revoked at any time for security reasons. Installation of any remote access equipment or technologies on any computing device requires approval from the Chief Information Officer (CIO) or his/her designee(s).

      (2) **Vendor Remote Diagnostics and Maintenance Access.** Temporary remote access privileges for vendors may be established by a system or firewall administrator with prior approval from the appropriate Reclamation Director or his/her designee(s). All temporary connections will be allowed only for the time period required to accomplish the approved tasks. All vendor activities will be monitored and logged during the time that any connection exists.

      (3) **Third-Party Access.** In strictly controlled situations, Reclamation allows third parties to access Reclamation internal networks and connected IT systems. A Memorandum of Understanding or an Interagency Agreement is required for access to Reclamation internal networks from external locations. Access by third parties will be strictly limited to the systems, facilities, and information needed to achieve predefined objectives. Access agreements will be reviewed annually to determine whether they need to be modified or continued. Network administrator(s) will periodically monitor third parties who have access to

Reclamation computers and networks to ensure compliance with this and other directives and standards.

B. **Authentication.**

(1) **Inbound Connections.** All IT system network connections initiated from a location outside an official Reclamation office or crossing a non-Reclamation network, and connecting to a Reclamation internal network, will employ approved authentication technology.

(2) **Outbound Connections.** IT system network connections initiated from inside an official Reclamation office do not need to employ authentication technology when connecting to a third-party network through Reclamation's IT security mechanisms.

C. **Connection Restrictions.**

(1) **Modems.** Modems in home-based, mobile, and/or telecommuting personal computers (PCs) are permitted for approved remote access. Modems in or connected to internal desktop PCs are not permitted without justification and prior approval of the appropriate Reclamation Director or his/her designee(s) and must adhere to the requirements of paragraphs 5B and 5C(2).

(2) **Inbound Dial-Up to Reclamation Networks.** All inbound dial-up lines connected to Reclamation internal networks and/or IT systems will pass through an approved Reclamation-managed security mechanism before users are permitted to reach a computer login banner. Exceptions to using Reclamation-managed security mechanisms may be requested from the CIO. Approval is contingent on the security method proposed.

D. **Link Requirements.**

(1) **Encryption.** Links between Reclamation and authorized third parties that transmit restricted or sensitive data will encrypt all data. Encryption will be accomplished using standards and tools agreed upon with the third-party partners and approved by the CIO or his/her designee. See Reclamation Manual (RM), *Information/Data Security*, IRM 08-11, for additional information.

(2) **Timeout After No Activity.** All IT systems accepting remote connections from public networks such as the dial-up phone network or the Internet will include a time-out system.

(3) **Connection Failure.**

(a) **Timeout on Connection Failure.** All IT systems with interfaces to external networks or systems will timeout a connection attempt if the attempt is not completed within a present period of time (typically 60 seconds).

(b) **Timeout Between Successive Unsuccessful Connection Attempts.** All IT systems with interfaces to external networks or systems will incorporate an assignable account/channel lockout after a fixed number of failed connection attempts by the external network or system. Any attempt to reconnect through the locked account/channel will be denied until the lockout is reset through either expiration of a lockout timer or an appropriately secure administrative means.

E. **No Trespassing Banners.** Where systems software permits, login banners will be used on all Reclamation networks and IT systems as defined in RM, *Computer Protection, Anti-Virus, Access Control, and Passwords*.

F. **Access Control to Third-Party Systems.** All Reclamation networks which are connected to third-party networks will employ access control to restrict the machines to which users can connect based on the business need for such access. Access control will be implemented via Reclamation-approved security mechanisms, processes, and procedures as defined in RM, *Configuration Management of Security Mechanisms*, IRM 08-03.

G. **Other Connections.** Establishment of any connection between a remote IT system used for Reclamation business activities and another network (such as Value Added Networks or personal Internet Service Providers) is prohibited unless prior approval from the appropriate Reclamation Director or his/her designee(s) has been obtained in writing. All Reclamation business, electronic mail, and web usage to and from non-Reclamation locations will be accomplished through an approved Reclamation-managed security mechanism.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the IT Security Program 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 the formation and coordination of processes to ensure remote access is adequate, appropriate, and supports Reclamation-wide IT security policy and standards. The ITSMs ensure compliance with remote access restrictions and requirements. The Bureau ITSM coordinates the activities of the ITSMs and acts as liaison to the Manager, Information Resources Services, or the CIO as appropriate.

D. **Administrators.** Administrators, such as Network Security Administrators, Remote Access Administrators, and Firewall Administrators maintain the reliability of Reclamation networks by ensuring remote access is adequate, appropriate, and supports Reclamation-wide IT security policy and standards.

E. **Reclamation Employees.** Reclamation employees are responsible for compliance with *IT Security Program* Directives and Standards in the RM, and those who willingly and deliberately violate them will be subject to disciplinary action identified in Public Law 99-474.

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