Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program (ITSP): Wireless Local Area Network (WLAN) Security

Purpose: Establishes the standards and requirements of protecting Reclamation Data and other IT resources for WLAN connectivity as part of the 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) Title X, Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); 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 (January 2000); Special Publication 800-10, *Keeping Your Site Comfortably Secured: An Introduction to Internet Firewalls*, National Institute of Standards and Technology; Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*; and DM Part 377, *Telecommunications*.

Contact: Chief Information Office, D-2200

1. **Introduction.** This Directive and Standard establishes the standards and procedures for the administration, control, operation, and maintenance of approved WLANs throughout Reclamation. Implementation of these guidelines will ensure secure access, transmission, operation, and maintenance for a WLAN environment.

2. **Goal.** The goal of this Directive and Standard is to:

   A. Establish guidelines to ensure secure wireless administration, operation, and maintenance;

   B. Protect Reclamation information, users, and wireless devices from unauthorized disclosure;

   C. Ensure protection against physical compromise;

   D. Establish guidelines for secure access through authentication and authorization mechanisms; and

   E. Establish guidelines for encrypting data between the wired network and wireless devices.

3. **Definitions.**

   A. **Access Point.** The wireless server that acts as a communication hub to connect clients to the internal network (also known as base station).

   B. **Network Device.** Any device that is traversed by data traveling from one device to another (not including the source/destination endpoints). Also included is any equipment that controls or monitors these devices or the data transmitted by them.

   C. **Service Set Identifier (SSID).** A 32-character, unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the network.

   D. **Wired Equivalent Privacy.** A security protocol for WLANs defined in the Institute of Electrical and Electronic Engineers 802.11b Standard.

   E. **Wireless Local Area Network (WLAN).** A type of local area network using high-frequency-radio waves to communicate between nodes.

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

   A. All Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., Supervisory Control and Data Acquisition Systems, Hydromet, Geographic Information Systems, and 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. **Requirements**

   A. **Transmission.**

      (1) WLAN devices may only be used to receive and transmit data defined as "Public" and "Sensitive" in Paragraph 3.C. of Reclamation Manual (RM), *Information/Data Security*, IRM 08-11, with procedure controls in Paragraphs 5.A.2. and 3. No "Restricted" data will traverse the WLAN. The "Restricted" definition is located in RM, *Information/Data Security*, IRM 08-11, Paragraph 3.A., with procedure controls in Paragraph 5.A.1.

(2) Direct data transmissions between wireless end user devices without first traversing a trusted network Access Point (i.e., ad-hoc configuration) are prohibited.

B. **Installation.**

(1) All Access Points must be authorized with proper approval(s) from the Regional IT Security Manager (ITSM) before it may be installed. Authorized installations shall be documented consistent with the guidance in the RM, *Network Systems*, IRM 08-02, Paragraphs 5.A.1., 2., and 3. Unauthorized installation is strictly prohibited.

(2) All procured WLAN devices (e.g., Access Points, network cards) must conform to all Reclamation ITSP Directives and Standards.

C. **Physical Implementation.**

(1) A firewall shall be placed between all Access Points and the wired network as described in Paragraph 5.C. of RM, *Network Systems*, IRM 08-02.

(2) Radio frequency transmission signals shall be minimized to reduce propagation of radio waves outside the facility or controlled area both horizontally, and, if applicable, vertically (e.g., to keep signals within the physical boundaries and not radiate past walls or defined controlled areas through the use of directional antennas or reducing the signaling power of the Access Point).

(3) Intrusion detection mechanisms shall be employed at the point of connection to the wired network, consistent with the guidance in Paragraph 5 of RM, *IT Intrusion Detection Systems*, IRM 08-06.

(4) Physically conceal Access Points whenever possible.

D. **User.** File sharing on all folders that contain documentation/information other than "Public" as defined in RM, *Information/Data Security*, IRM 08-11 shall be disabled.

E. **Authentication and Encryption.**

(1) A user authentication mechanism such as a username/password, smart card, or security token shall be employed to properly identify authorized end users.

(2) Static internet protocol addresses for wireless clients and Access Points (i.e., disable dynamic host configuration protocol) shall be utilized.

(3) To encrypt transmitted data between wireless devices and Access Points, at a minimum 802.11 wired equivalent privacy with 128-bit encryption must be activated and enforced.

F. **Administration and Maintenance.**

(1) A list of authorized users and their radio network interface cards and/or Media Access Point (MAC) addresses shall be maintained.

(2) MAC address authentication via access control lists. Access Points will be set up to allow only clients/users with specific MAC addresses to access the network or allow access to only a given number of MAC addresses.

(3) WLAN devices will be turned off during non-business hours (6 p.m. to 6 a.m.). Offices that operate in a 24-hour environment will document their requirement and request an exception via the procedures outlined in Paragraph 5 of RM, *Remote and Third-Party Access*, IRM 08-10.

(4) Default passwords shall be changed and strong passwords shall be implemented consistent with the guidance in RM, *Computer Protections, Anti-Virus, Access Control, and Passwords*, IRM 08-12. In particular, the settings for the following shall be changed:

(a) Access Point SSID name;

(b) Simple network management protocol community strings (passwords); and

(c) Administrator account password.

(5) For all Access Points:

(a) The broadcast SSID feature shall be disabled.

(b) The access device default channel shall not be used.

(c) The SSID shall not be set to a NULL value to prevent access or from accepting connections from unauthorized users/devices.

(d) Responding to probe requests to retrieve the SSID shall be disabled.

(e) HTTP and SNMP interfaces will be disabled after initial configuration.

(6) A dynamic key exchange mechanism shall be utilized.

(7) Network interface cards and Access Point firmware shall be periodically updated to ensure the latest firmware releases and patches are implemented.

(8) Only authorized personnel shall reset the Access Points. If an Access Point can be reset via a recommended standard-232 cable through a console connection, the console port shall be disabled.

(9) Operational support tools shall be utilized to monitor for rogue Access Points that do not conform to configuration policies. Rogue Access Points shall be shut down when identified.

(10) On a periodic basis, routine audits shall be performed to detect exceptions or abnormal network activities and an alert shall be sent to network administrators.

G. **General.**

(1) All existing Reclamation 802.11 wireless systems are required to be evaluated to determine if they meet the approved operational standards.

(2) Any WLAN equipment not meeting the above conditions is unauthorized for use and will be immediately turned off to prevent possible intrusion.

(3) Handheld devices using a cellular/personal communications service/cellular digital packet data/baseband pulsed radar sensor network will be addressed under separate policy since they involve different technologies and issues.

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 Directors/Managers in the formation and coordination of processes to ensure the network security architecture is adequate, appropriate, and supports 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. **Reclamation Employees.** Reclamation employees are responsible for compliance with ITSP Directives and Standards, 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 section of the RM.