NASA Standard Operating Procedure

Wireless Local Area Network Implementation

ITS-SOP-0020 (assigned by the OCIO)
Version: 20051005
Effective Date: 20051005
Expiration Date: 20071005
Responsible Office: OCIO / Chief Information Officer

REVISION RECORD

ITEM NO.	REVISION	DESCRIPTION	DATE

Wireless Local Area Network Implementation

Objective: The use of wireless local area networks (WLANS) provides wider capability to access the wired network through mobile computing devices. However, with the added benefits of wireless networking also comes additional risk. If implemented without the appropriate security controls, a wireless network can easily be exploited and used as a conduit for unauthorized network access, misuse, and abuse. Those responsible for the installation and operation of a wireless network must be aware of the inherent risks that exist in a wireless environment and its impact on a Center's Information Technology (IT) security posture. This SOP provides guidance on properly implementing security for WLANs.

Reference: Specific guidance for WLANs can be found in NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices
Procedures

1.0 Implementation

a. NASA shall follow the guidance provided by NIST Special Publication 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

b. The design architecture for all WLANs shall provide for an association between a specific access point and a connection to the wired LAN.

c. WLAN resources shall be treated as part of network infrastructure following all existing security and network standards, policies and procedures.

(1). WLANs shall be prohibited as the sole or primary means of access where the availability of a system or system information is identified as a moderate or high security risk category unless protected through the use of FIPS 140-2 compliant encryption.

c. Wireless networks and/or wireless access points shall be:

(1). Prohibited on a NASA's mission critical Internet Protocol Operational Network.

(2). Confined to logically or physically isolated networks or connected to a Center's open network.

(3). Approved for legal conformance by the Center Frequency Manager prior to the purchase of the wireless equipment.

(4). . Encrypted utilizing a dynamic link that is unique for each user and session.

Wireless networks and/or wireless access points shall be:

(5). Prohibited on a NASA's mission critical Internet Protocol Operational Network.

(6). . Confined to logically or physically isolated networks or connected to a Center's open network.

(7). Approved for legal conformance by the Center Frequency Manager prior to the purchase of the wireless equipment.

(8). Encrypted utilizing a dynamic link that is unique for each user and session.

e. Authentication and authorization access to wireless networks shall:

(1). Be approved by the Center NCCB for access points and wireless devices.

(2). Provide authentication that utilizes NASA-approved encryption protocols to ensure confidentiality of authenticating information or other authentication approaches approved by the Center NCCB.

(3). Provide individual accountability for each user accessing WLAN resources.

(4). Provide for strong authentication where feasible.

(5). Provide for the confidentiality of wireless data transmission.

2.0 Moderate and High Networks

a. WLANs shall be prohibited as the sole or primary means of access where the availability of a system or system information is identified as a moderate or high security risk category unless protected through the use of FIPS 140-2 compliant encryption (see chapter 12).

b. Wireless networks and/or wireless access points are prohibited on a Center's private network unless protected through the use of FIPS 140-2 compliant encryption.

c. Adhoc networks are prohibited.

3.0 Transmission of Sensitive data

a. Wireless transmissions of ACI or SBU data are prohibited unless the wireless network's transmission is performed using Center-approved encryption protocols.

4.0 *Management*

a. All WLANs shall be managed by the Center NCCB to include:

(1). Approval and documentation all network management protocols to be allowed for use on wireless local area network (WLAN) access points, including approval of installation and use of all WLAN access point equipment, configuration, and security controls.

(2). Maintenance of a list of authorized wireless equipment that has been verified by the Center Frequency Manager.

(3). Verification that wired equivalent privacy (WEP) and server set identification (SSID), static WEP keys and SSID, Wi-Fi Protected Access (WPA and WPA2), and MAC address filtering are not the only security measures for a WLAN.

(4). Verification that WLAN access points are physically secured and administrative logons are secured to prevent unauthorized tampering or access to the devices.

(5). Verification that the radio frequency (RF) transmission footprints of the WLAN access points are limited to the greatest extent possible to areas where authorized users are expected to reside.

(6). Verification that the WLAN access points with connectivity to Center-wired networks that are established on the Center registered IP addresses.

(7). Verification that WLAN access points and IP addresses are registered with the Center NCCB and comply with IP address management requirements.

(8). Access to wireless network access points shall be limited to authenticated users and approved wireless devices, which are authorized by the Center's Network Configuration Control Board (NCCB).

5.0 Monitoring

a. The WLAN shall be monitored:

(1). On a regular basis for security, performance, traffic analysis, and vulnerabilities.

(2). For unusual or suspicious activity by reviewing authentication, authorization, and usage logs.

(3). For any unusual events that reflect unauthorized use and immediately be reported to the Center ITSM.

b. A full Center site survey shall be performed at least semi-annually to detect unauthorized WLAN access points. Spot checks for unauthorized WLAN access points shall be performed quarterly.

6.0 Waivers

a. Waivers for special circumstances shall be submitted for consideration to the Center NCCB and approved or disapproved by the Center CIO on a case-by-case basis. A security assessment and impact report shall be required for all waivers and documented in the appropriate SSP.

S. Scott Santiago ______________ 10/5/2005

S. Scott Santiago
Deputy Chief Information Officer
Information Technology Security

Date