Information System Security
Wireless Access Standards and Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mbg_060106_cd44

Information System Security
Wireless Access Standards and Guidelines
for System Owners, ISSOs, and System Administrators

Wireless technologies have become increasingly popular in every day business and personal life. Laptops and personal digital assistants (PDAs) allow individuals to access calendars, e-mail, address books, and the Internet. Wireless technologies promise to offer even more features and functions in the next few years.

You should be aware that there are security risks associated with wireless technologies and you must take care when using wireless devices. As a System Owner, you must develop strategies that will mitigate identified risks as you integrate wireless technologies into any USAID information system or computing environment. You must have CISSO approval to deploy any wireless technology.

You must ensure that wireless networks comply with **all** items in the **Security Preconditions *and*** the **Security Standards** checklist sections before being placed into operation. If you cannot make the wireless network comply, then you must not place the wireless network into operation. If possible, you should comply with the items appearing in the Security Recommendations section.

Within this document's scope, wireless clients are any desktop, laptop, and Blackberry devices with wireless capability (802.11 or Blackberry compliance).

Wireless LAN Security Checklist

The following table provides a security checklist for wireless local area networks (WLANs):

Item #	Security Preconditions Wireless networks must comply with these standards in order to operate.	Status
1	**Install a properly configured firewall between the wired infrastructure and the wireless network (access point or hub to access points).**	
2	**Install anti-virus software on all wireless clients.**	
3	**Install personal firewall software on all wireless clients.**	
Item #	**Security Standards** Wireless networks must comply with the below standards before operation.	**Status**
1	**Maintain a complete inventory of all 802.11 wireless devices (active and inactive).**	
2	**Change the default service set identifier (SSID) in the access points.**	
3	**Validate that the service set identifier character string does not reflect USAID's name (division, department, etc.).**	
4	**Review, and where necessary, change default parameters.**	
5	**Disable all insecure and nonessential management protocols on the access points.**	
6	**Enable all security features of the WLAN product, including the cryptographic authentication and wireless encryption protocol (WEP) privacy feature.**	
7	**The encryption key size must be at least 128-bits.**	
8	**Replace the default shared keys, and change them every 90 days.**	

9	**Deploy media access control (MAC) lists.**	
10	**All wireless device passwords must meet or exceed USAID password standards.**	
11	**Disable the "ad hoc mode" for 802.11. If you cannot disable this feature; use a different vendor.**	
12	**Disable dynamic host control protocol (DHCP), use static IP addressing.**	
Item #	**Security Recommendation**	**Status**
1	Perform a risk assessment to understand the additional risks that wireless access presents.	
2	Upgrade the client network interface card and access point support firmware as patches become available.	
3	Perform comprehensive security assessments at least quarterly (including validating that rogue access points do not exist in the 802.11 WLAN).	
4	Ensure that external boundary protection is in place around USAID building perimeters.	
5	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	
6	Complete a site survey to measure and establish the access point coverage.	
7	Locate access points on building interiors instead of near exterior walls and windows.	
8	Place access points in secured areas to prevent unauthorized physical access and user manipulation.	
9	Empirically test access point range boundaries to determine the precise extent of the wireless coverage.	
10	Make sure that the reset function on access points is used only when needed and is only invoked by authorized personnel.	
11	Restore the access points to the latest security settings when the reset functions are used.	
12	Disable the broadcast service set identifier feature so that the client service set identifier matches that of the access point.	
13	Ensure that access point channels are at least five channels different from any other nearby wireless networks to prevent interference.	
14	Disable file sharing on wireless clients (especially in untrusted environments).	
15	Consider installing Layer 2 switches instead of hubs for access point connectivity.	
16	Deploy IPSec-based virtual private network (VPN) technology for wireless communications.	
17	Ensure that the encryption used is sufficient given the data sensitivity on the network.	
18	Fully test and deploy software patches and upgrades on a regular basis.	
19	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.	
20	Enable user authentication mechanisms for the management interfaces of the access point.	
21	Ensure that management traffic destined for access points is on a dedicated wired subnet.	
22	Use secure network management protocol (SNMP) v3 and/or secure sockets layer/transport layer security (SSL/TLS) for web-based management of access points.	
23	If used, configure SNMP settings on access points for least privilege (i.e., read only). Disable SNMP if it is not used.	
24	Use a local serial port interface for access point configuration to minimize the exposure of sensitive management information.	
25	Deploy intrusion detection agents on the wireless network to detect suspicious behavior or unauthorized access and activity.	
26	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	
27	Enable key-mapping keys (802.11) rather than default keys so that sessions use distinct WEP keys.	
28	Review the impacts of deploying any security feature or product prior to deployment.	

29	Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.	
30	When disposing of access points that will no longer be used by USAID, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	
31	If the access point supports logging, turn it on and review the logs on a regular basis.	

This table is a security checklist for wireless local area networks.

Wireless Client Security Checklist

The following table provides a security checklist for wireless clients:

Item #	Security Standards Wireless clients must comply with the below standards.	Status
1	**Wireless device users must be able to securely authenticate when operating remotely.**	
2	**Enable a "power-on" password for each handheld device.**	
Item #	**Security Recommendation**	**Status**
1	Perform a risk assessment to understand the additional risks that wireless access presents.	
2	Conduct ongoing, random security audits to monitor and track devices.	
3	Ensure that external physical boundary protection is in place around USAID building perimeters.	
4	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	
5	Ensure that users know how to report a lost or stolen device.	
6	Ensure that devices are stored securely when left unattended.	
7	Make sure that add-on modules are adequately protected when not in use to prevent theft.	
8	Ensure proper password management (aging, complexity criteria, etc.) for all handheld and laptop devices.	
9	Ensure that desktop access application-mirroring software is password protected.	
11	Review vendor web sites frequently for new patches and software releases.	
12	Install patches on the affected devices and workstations.	
13	Review security-related mailing lists for the latest security information and alerts.	
14	Ensure that all devices have timeout mechanisms that automatically prompt the user for a password after an inactive period.	
15	Sensitive information must not be placed on PDAs.	
16	Turn off communication ports when not in use.	
17	Ensure that PDAs are provided with secure authorization software/firmware.	
18	Install virtual private network (VPN) software on all handheld devices that transmit data wirelessly.	
19	Use robust encryption and password protection utilities for protecting sensitive data files and applications.	
20	Use enterprise security applications to manage handheld device security.	
21	Ensure that security assessment tools are used on handheld devices.	
22	When disposing of handheld devices that will no longer be used by USAID, clear configuration settings to prevent the disclosure of sensitive network information.	

This table is a security checklist for wireless clients.

REFERENCES

NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices, November 2002.