WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 4, Release 1

31 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

TABLE OF FIGURES

This page is intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES

The previous release was Version 3, Release 1, dated 15 April 2004.
All technology sections have been renamed and reorganized significantly to accommodate the changes in technology. The functionality of wireless devices is no longer as clear-cut and many products perform multiple functions.

SECTION CHANGES

SECTION 1. INTRODUCTION

Moved the wireless security discussion to *Section 2.1*.
Added reference to wireless wide area networks (WWANs) to third paragraph in *Section 1.1*.
Added reference to Knowledge Management Web site to Paragraph 4. Major editing throughout *Section 1.1*. In *Section 1.6* and *1.7* changed URLs and contact information.

SECTION 2. WLAN, WPAN AND WWAN TECHNOLOGIES

Major editing throughout this section. Subsection titles changed throughout. WIR0010, WIR0012, WIR0040, WIR0090, WIR0270, and WIR0290 updated/clarified throughout. WIR0320 deleted throughout this section.

Section 2.1 Introduction

Added a new introductory paragraph.

WIR0010 reworded to make the requirement applicable to WLAN, WPAN, and WWAN systems.

WIR0015 reworded to make the requirement applicable to WLAN, WPAN, and WWAN systems. Updated/added requirements for wireless hardware list.

WIR0060 reworded to make the requirement applicable to WLAN, WPAN, and WWAN systems.

WIR0080 deleted. Upgraded WIR0010 to CAT I and WIR0015 to CAT III. Added WIR0075, CAT III regarding periodic screening for rogue access devices.

Section 2.2 IEEE 802.11 WLAN System

Added subparagraphs for 802.11f and 802.11g protocols. Edited subparagraph for 802.11i protocol.

Added WIR0460, which requires protection of data at rest.

Section 2.2.1.2 Access Points

Added WIR0140, WIR0150, WIR0250, and WIR0290 which were pre-existing compliance requirements.

Section 2.2.2.2 IEEE 802.11 WLAN Topologies

Updated WIR0125 with the word “strong.”

Section 2.2.3.1 Services Set Identifier (SSID)

WIR0140 updated with phrase “upper and lower case.”

Section 2.2.3.2 MAC Address Filtering

WIR0160 downgraded to CAT III.

Section 2.2.4 Security Issues with Windows 200, XP and Embedded Wireless Systems

Removed reference to Draft CNSS 3034 and added reference to SWLAN Addendum. Updated information on SecNet 54. WIR0204 (CAT I) updated with more details on compliance requirements. Added existing WIR0040. Added new requirement WIR0206 (CAT III) requiring written operating procedures for managing hardware and key materiel for SWLANs.

Section 2.2.5 IEE 802.11 WLAN Implementation Compliance Requirements

Updated technical information on Windows XP and 2000 features. Added subsections to make the requirements for Windows with and without the appropriate service pack updates. WIR0163, and WIR0164 updated. WIR0168 (CAT III) added regarding Windows XP, SP2 WZC service’s Preferred Network connection setting. WIR0070 upgraded to CAT III.

Section 2.2.5.1Classified WLAN Systems

WIR0180 (CAT II) added DCID approval requirement.

Section 2.2.5.2 Unclassified WLAN Systems

Upgraded WIR0160 to CAT III. WIR0260 (CAT II) WIR0270 (CAT II), and WIR0290 wording updated to clarify policy. WIR0161 (CAT II) added.

Section 2.2.5.1

Updated first paragraph. WIR0170 and WIR0180 are minor updates. Added WIR0204, WIR0040, and WIR0206 to this section from Section 2.2.3.4. Replaced the first instance of NET0210 with WIR0205.

Section 2.3.1 Bluetooth Compliance Requirements

Updated Bluetooth technology overview. Added Figure 2-4.

Section 2.3.1.1 Classified Information

Changed WIR0181, WIR0182, WIR0225 to CAT I. Added WIR0009 (CAT I) regarding DAA approval for wireless systems processing classified information. Upgraded WIR0181 to CAT I from CAT II and added DCID requirement to the policy.

Section 2.4. Wireless Mice and Keyboards

Deleted WIR0010 from this section. Added WIR0131 (CAT II) regarding use of IR keyboards and mice. Updated WIR0132 to add WLAN and Bluetooth mice to the requirement.

Section 2.6. **WWAN Technologies, Protocols, and Security**

This section on WWAN technologies and security requirements was moved from Section 3. The word broadband was generally changed to WWAN throughout.

Section 2.6.5.1 Classified Broadband Wireless Systems

Upgraded WIR0373, WIR0374, and WIR0375 to CAT I from CAT II.

Section 2.6.5.2 Unclassified WWAN Systems

Changed WIR0377 to CAT III to CAT II to match WIR0270.

Added Section 2.7, discussing RFID technologies.

SECTION 3. WIRELESS PED TECHNOLOGIES

This section was renamed. Information about PDAs, telephones, SMS and e-mail devices was combined into one section. This information was previously in Section 4, which was removed.

Section 3.1 Introduction

Major rewording and reworking.

Section 3.2.5.1 Classified Information

Upgraded WIR0350 to CAT I, regarding use of Type 1 devices for classified voice.

Section 3.2.5.2 Unclassfied Information

Added WIR0340 (CAT III) regarding user training. Added last paragraph regarding cellular voice encryption.

Section 3.3.4.1 Classified Information

Changed WIR0010 to WIR0009 and updated to CAT I. Upgraded WIR0380, WIR0390, and WIR0400 to CAT II from CAT II. Added pre-existing WIR0180 (CAT II) to this section. Upgraded WIR0410 to CAT I and updated wording to remove the acronym “SCIF.” Upgraded WIR0356 to CAT I, regarding PDAs with digital cameras.

Section 3.3.4.2, **Unclassified Information**

Changed WIR0010 to WIR0012 and updated to CAT I regarding DAA approval of applications, connections and services. Changed WIR0010 to WIR0011 (CAT II) regarding use of personally owned equipment. Updated WIR0050 to replace DOD CERT with JTF-GNO. Changed first instance of WIR0480 to new number, WIR0479 and upgraded the new policy to CAT II from CAT III.

Section 3.4.2

All subsections removed and relocated to Appendix C, BlackBerry Security.

Section 3.2.6 Blackberry Wireless Two-way E-mail

Added a subsection referencing the new BlackBerry Security appendix.

APPENDIX A. RELATED PUBLICATIONS

Verified all HTML links are still valid.

Reference information for the following publications were updated: OMB Circular A-130; DODD 8100.1.

Reference information for the following publications or references was added: FWUF organization added to Government Agencies section.

APPENDIX B. IAVM COMPLIANCE

Chart of existing vulnerabilities added.

APPENDIX C. BLACKBERRY SECURITY

Removed former Appendix C, Wireless LAN Site Survey Guide. Now known as Wireless LAN Site Survey Guide Addendum to the Wireless STIG.

Newly added appendix with content moved from previous Section 3.4, Wireless Two-ay E-mail.

Major editing and technology updates throughout. Major policy changes. This section was made more generic by removing references to RIM 957-8 model. BES version 4.0 features addressed.

Section C.2.1 Classified Information

Upgraded WIR0500, WIR0360, and WIR0520 to CAT I from CAT II. Added new requirements WIR0592 (CAT III) and WIR0593 (CAT I).

Section C.2.2 Unclassified Information

Updated WIR0050 to replace DOD CERT with JTF-GNO. WIR0610 (CAT II) deleted. Deleted WIR0600 as this is a duplicate requirement. Updated WIR0620 requiring use of kill command for lost devices. Updated and upgraded WIR0593 (CAT I) regarding MDS configuration. Major changes to WIR0630 which now defines minimum password configuration requirements for the BlackBerry. Added WIR0640 (CAT II) regarding use of Bluetooth on BlackBerry devices.

APPENDIX D. LIST OF ACRONYMS

Removed former Appendix D and renamed as the WLAN Reference Model Addendum to the Wireless STIG.

Updated throughout with new acronyms.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This *Wireless Security Technical Implementation Guide* (STIG) is published as a tool to assist in the improvement of the security of Department of Defense (DOD) commercial wireless information systems. The document is meant for use in conjunction with the *Network STIG* and appropriate operating system STIGs.

Use of wireless technologies can improve productivity of DOD employees; however, wireless systems and handheld devices may also introduce security vulnerabilities, which, if left unmitigated, can expose government information systems to attack. In the last five years, there has been a dramatic evolution in wireless technologies, standards, and implementation practices. These changes impact the security of both wireless and wired networks. The pace of these changes is not expected to decrease for the foreseeable future, therefore solid security engineering practices and wireless network implementation policies are crucial to ensure that DOD wireless systems are deployed and operated in a secure manner. To that end, this STIG provides an overview of each wireless technology and the security impact associated with incorporating these wireless devices into the DOD environment.

This STIG supports the design, implementation, and management of wireless devices and networks that are used to provide e-mail and other information technology services to mobile workers in the DOD and provides implementation guidance for DOD Directive 8100.2. Additional information on wireless systems can be found on the DOD Wireless Community of Practice Knowledge Management (CoP KM) Web site at http://acc.dau.mil. Select the “DOD Wireless” workspace from the main web page.

This document does not cover every wireless system or network in use, or being considered for use, in the DOD. The target is for commercial wireless systems, networks, and devices that are used to provide office environment type services (e.g., e-mail, travel applications, connections to office networks) using commercially available wireless equipment and wireless carriers. The intent is for the requirements in this STIG to supplement other OS and network STIGs so that a seamless security infrastructure can be maintained within the DOD enterprise.

In an effort to ensure that the STIG reflects the latest wireless technology, usage trends, and DOD wireless policies and guidance, the document is updated on at least an annual basis. In this version you will find that *Sections 2, 3,* and *4* from previous versions have been reorganized into two sections to reflect the convergence of cell phones, PDAs, messaging devices, and wireless email devices into one handheld device.

Section 2, WLAN, WPAN, and WWAN Technologies, discusses Wireless Local Area Networks (WLAN), Wireless Personal Area Networks (WPAN), and Wireless Wide Area Networks (WWAN) (wireless broadband) network technologies and security policies. In addition, this section addresses Radio Frequency Identification (RFID) systems. Security requirements for Personal Electronic Devices (PED), including cell phones and PDAs are discussed in *Section 3, Wireless PED Technologies*. *Appendix C, BlackBerry Security*, provides procedures for securing the BlackBerry wireless email device.

A new feature of the *Wireless STIG*, starting with this version, is the *Wireless STIG* addendums. The addendums are designed as stand alone security guidance documents that provide an in-depth discussion of a particular wireless security topic area. The following *Wireless STIG* addendums are available on the IASE web sites:

- *Wireless LAN Security Framework Addendum*
- *Mobile and Wireless device security Guidance Addendum*
- *Secure Wireless Local Area Network Addendum (access only to* ***.mil*** *or* ***.gov*** *addresses)*
- *Wireless LAN Site Survey Addendum*

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

This document is a requirement for all DOD administered systems and all systems connected to DOD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1 Vulnerability Severity Code Definitions

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. WLAN, WPAN, AND WWAN Technologies

2.1 Introduction

The following subsections describe the technology and security issues involved with DOD use of wireless networking devices such as WLANs, WPANs, WWANs, and RFID. These technologies provide authorized users with wireless access to wired network resources, including the Internet.

WLANs are generally developed as an extension to an existing wired infrastructure, although they may be installed as standalone as well. WPANs operate in the Personal Operating Space (POS) of a user, which extends 10 meters in any direction. WWAN systems are typically systems that provide wireless broadband data services. These systems include Broadband Wireless Access (BWA), Mobile Broadband Wireless Access (MBWA), and cellular 3G (third generation) data systems.

Wireless networking technologies may also be divided into short-range and long-range standards. Short-range (less than one mile) wireless standards development has occurred in three systems—Institute of Electrical and Electronics Engineers (IEEE) 802.11 (WLAN), IEEE 802.15 (Bluetooth), and IEEE 802.16 (BWA). Long-range commercial standards development has occurred primarily in cellular 3G systems. The technology overview of cellular 3G systems is located in *Section 3.2, Cellular Technologies, Protocols, and Security*. However, the cellular 3G security requirements are the same as WWAN systems and are, therefore, located in *Section 2.6, WWAN Technologies, Protocols, and Security*.

The mobility and transmission methods used for WLANs, WPANs, and WWANs introduces security issues when used as part of or close to the DOD Enclave. To ensure security in today's wireless environments, the IAO must ensure that wireless systems (WLAN, WPAN, and WWAN) are designed using a defense-in-depth approach using multiple layers of security as described in *Section 2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements*. The following requirements apply to all wireless systems:

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0012: CAT I) The IAO will ensure only DAA approved peripheral devices, operating systems, applications, and network/PC connection methods and wireless services are used.*

- *(WIR0015: CAT III) The IAO will maintain a list of all DAA approved wireless devices. For WLAN devices, the list includes the following:*

  - *Access point Media Access Control (MAC) address*
  - *Access point IP address*
  - *Wireless client IP address*
  - *Wireless client MAC address*
  - *Wireless channel set for each access point*

- *Access point DHCP range*
- *Type of encryption enabled*
- *Encryption key used*
- *Access point SSID*
- *Manufacturer, model number, and serial number of wireless equipment*
- *Equipment location*
- *Assigned users with telephone numbers*

- *(WIR0075: CAT III) The IAO will ensure a policy is in place to periodically scan for rogue wireless devices.*

  - *(WIR0030: CAT III) The IAO will ensure wireless devices connecting directly or indirectly (hot-sync) to the network are added to the site System Security Authorization Agreements (SSAA).*

  - *(WIR0060: CAT II) The IAO will ensure wireless systems (WLAN, WPAN, and WWAN) are compliant with overall network security architecture, appropriate enclave security requirements, and DODD 8100.2 before the system is installed.*

2.2 IEEE 802.11 WLAN Systems

The Institute of Electrical and Electronic Engineers (IEEE) 802.11 standard defines the interoperability requirements for WLANs operating in the 2.4 and 5 GHz unlicensed bands. Products using the 802.11b standard operate in the 2.4 GHz band at a maximum data rate of 11Mbps. Products using the 802.11a standard operate in the 5 GHz band with a data rate of up to 54 Mbps. Products implementing the 802.11g standard operate in the same frequency range as 802.11b equipment but at a data rate of up to 54 Mbps.

The IEEE 802.11 standards group defines the WLAN standard. There is a sub-committee or sub-group for each component of the 802.11 standard.

- IEEE 802.11a is the standard for high speed WLANs in the 5 GHz band. The standard defines data rates between 6-54 Mbps with 6, 12, and 24 Mbps required for any implementation.

- IEEE 802.11b is the standard for WLANs in the 2.4 GHz band. The standard defines 1, 2, 5.5, and 11 Mbps data rates.

NOTE: A number of WLAN vendors have released IEEE 802.11b WLAN products that can operate at 22 Mbps data rates. These products are based on proprietary extensions to the IEEE 802.11b standard and will not interoperate with other standard 802.11b products when set to use 22 Mbps. However, these products can dynamically adjust to operate at standard 802.11b data rates to support multi-vendor environments.

- IEEE 802.11e is a developing standard that will specify Quality of Service (QoS) for WLAN systems that require QoS support (e.g., Voice over Internet Protocol (VoIP) WLAN systems).

- IEEE 802.11f is the standard for the Inter-Access Point Protocol – IAPP, defines roaming compatibility across access points from different vendors.

- IEEE 802.11g is the standard for high speed (up to 54 Mbps) WLANs in the 2.4 GHz band.

NOTE: A number of WLAN vendors have released "Super G" WLAN systems, which operate at 104 Mbps. Super G products are based on proprietary extensions to the IEEE 802.11g standard and will not interoperate at 104 Mbps with other vendors' Super G systems (but can dynamically adjust to operate at standard 802.11b/g data rates with other 802.11b/g WLAN systems).

- IEEE 802.11h is a developing standard that specifies dynamic channel selection and transmission power control for WLAN systems. Its purpose is to minimize interference between IEEE 802.11a WLAN systems and other systems operating in the 5 GHz frequency band such as radar systems, Earth Exploration Satellite Service (EESS) systems, and Space Research Service (SRS) systems.

- IEEE 802.11i is the new security specification of the 802.11 standard and consists of two components: IEEE 802.1x and Robust Security Network (RSN). See *Section 2.2.3.4, Wi-Fi, WPA, and RSN,* for a description of RSN.

- IEEE 802.11j is the standard for WLAN systems operating in the 4.9 – 5 GHz frequency band in Japan.

- IEEE 802.11n is a developing WLAN standard that will provide data rates in excess of 100 Mbps.

- IEEE 802.1x is the Port Based Network Access Control standard. Included in the IEEE 802.1x standard is Extensible Authentication Protocol (EAP), which provides multiple user-based authentication methods (smart cards, Kerberos, Public Key Infrastructure (PKI), etc.). EAP provides a standard method for user authentication in WLAN systems. Various WLAN vendors have implemented proprietary versions of EAP. The most common versions of EAP include the following:

  - EAP-Transport Layer Security (EAP-TLS) provides very strong security, but requires use of a client certificate. Used primarily in enterprises that already have deployed a PKI infrastructure. EAP-TLS provides for certificate-based, mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication; dynamically generated user- and session-based keys are distributed to secure the connection. Windows XP includes an EAP-TLS client.

  - EAP-Tunneling Transport Layer Security (EAP-TTLS) is an extension of EAP-TLS, which provides for certificate-based, mutual authentication of the client and network. Unlike EAP-TLS, however, EAP-TTLS requires only server-side certificates, eliminating the need to configure certificates for each WLAN client. EAP-TTLS uses TLS records to tunnel the client authentication.

- Protected Extensible Authentication Protocol (PEAP) is similar to EAP-TTLS; however, with PEAP, only EAP may be carried as a protocol inside the tunnel.

- Lightweight Extensible Authentication Protocol (LEAP) is used primarily in Cisco WLAN access points. It encrypts data transmission using dynamically generated WEP keys, and supports mutual authentication.

- EAP-MD-5 provides only minimal authentication capability and is not recommended because of significant security vulnerabilities. EAP-MD-5 duplicates CHAP password protection.

2.2.1 IEEE 802.11 WLAN Components

To understand WLANs and their associated security, you should understand the two basic elements of a wireless network, namely, the wireless station and the access point.

2.2.1.1 WLAN Stations/Clients

A wireless station can be a laptop, desktop PC, handheld device, access point, or any other device that utilizes wireless communication as a means of communicating with other network devices. Stations may be mobile, portable, or stationary and can be used to transmit data or voice (e.g., VoIP phones). Wireless network interface cards (NICs) are manufactured in the same form factors as their wired counterpart (e.g., Personal Computer Memory Card International Association (PCMCIA) cards, Peripheral Component Interconnect (PCI) cards, Industry Standard Architecture (ISA) cards, Compact Flash (CF) cards, Universal Serial Bus (USB) cards).

The requirements for wireless stations are as follows:

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs, if available.*

NOTE: Most wireless LAN bridges can connect to both clients and other bridges. If a WLAN bridge is configured to allow connections to WLAN clients, the bridge should be configured IAW *Section 2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements*.

- *(WIR0090: CAT II) The IAO will ensure an access control mechanism is placed on all 802.11-enabled devices.*

- *(EN785: CAT III) The IAO will ensure a policy is in place to periodically scan for rogue wireless devices.*

NOTE: Organizations are required to scan for unauthorized wireless devices, regardless of whether they have a WLAN installed.

- *(WIR0460: CAT II) The IAO will ensure tools are used to encrypt data at rest on the wireless device. Encryption tools must be FIPS 140-2 certified.*

2.2.1.2 Access Points

An access point is the entry point from a wireless station to a WLAN, from a WLAN to a wired LAN, or between WLANs. Access points generally consist of a radio, a wired network interface, and management and bridging software. Access point functionality can be implemented using a hardware device or an application installed in another network device (a router for example) and is configured based on architecture requirements. Some vendors have removed the management and bridging software from the access point and placed these features into a wireless switch and then all access points on the network are managed and configured from the wireless switch. In a WLAN system with wireless switches, the access points are usually called access ports and are essentially transceivers (transmitter/receiver of data) with a network interface.

- *(WIR0140: CAT III) The IAO will ensure SSIDs are changed from the manufacturer's default to a pseudo random word consisting of a combination of upper and lower case characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure the SSID broadcast mode is disabled. WLANs that do not allow the SSID broadcast mode to be disabled will not be used.*

- *(WIR0250: CAT II) The IAO will ensure the WLAN access point is set to the lowest possible transmit power setting and meets the required signal strength of the area serviced by the access point.*

- *(WIR0290: CAT II) The IAO will ensure access points and bridges are placed in a screened subnet (DMZ on firewall separating intranet and wireless network), or Virtual LAN (VLAN) and or otherwise separated from the wired internal network. A VPN concentrator or wireless security gateway/switch is placed between the access point and the local DOD network.*

NOTE: The wireless network must be separated from the wired network using an authorized architecture as described in WIR0290. The wireless DMZ is not the same as the enclave DMZ.

2.2.2 Technology Overview

WLANs may utilize infrared (IR) technology, narrowband technology, or radio frequency (RF) transmission. Data is placed onto a radio wave through a process called modulation, and the carrier wave acts as the transmission medium (replacing the copper or fiber optic cable of the wired network). In addition to the 2.4 GHz Industrial, Scientific, and Medical (ISM) band, WLAN products are also available that operate in the 5 GHz Unlicensed National Information Infrastructure (UNII) band (IEEE 802.11a).

2.2.2.1 Data Transmission

WLANs transmit and receive data using several different methods. IEEE 802.11b standard defines three different physical layers—Baseband Infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). The IEEE 802.11a and 802.11g standards specify orthogonal frequency division multiplexing (OFDM) as the transmission method.

2.2.2.1.1 Infrared

Infrared-based WLANs are best suited for wireless networks whose requirements are for use within a small group or subnetwork. Infrared signals do not penetrate solid objects, such as walls and floors in a building. There are few commercial implementations of infrared WLANs because access points and stations must be within line of sight when using this transmission method.

Most commercially available infrared transceivers produce a signal even when the device is turned off via software. Covering the transceiver with metallic tape or placing the wireless device into a container with electromagnetic shielding can secure infrared transceivers.

- *(WIR0110: CAT III) The IAO will ensure infrared WLAN receivers and transmitters are disabled when not required. The local Certified TEMPEST Technical Authority (CTTA) should be consulted to determine appropriate methods for disabling a specific Infrared wireless device.*

2.2.2.1.2 Spread Spectrum

Most WLANs use spread spectrum technology for transmission. There are two methods used for spred spectrum, FHSS and DSSS. FHSS transmissions jump between several frequencies at a pre-determined rate/interval. DSSS uses a redundant chipping code. DSSS is used by nearly all 802.11b wireless LAN radios. Radio waves using the 802.11b standard, which operates at 2.4 GHz, can easily penetrate building walls and have a coverage range of up to a few hundred feet, which is useful when the signal must traverse large areas, such as multi-floor and campus environments. FHSS and DSSS do not interoperate; the transmitter and the receiver must be configured for the same transmission method.

2.2.2.1.3 OFDM

OFDM is the modulation scheme used by 802.11a and 802.11g WLANs. This method transports data using many carrier waves, with each wave carrying part of the message. The OFDM method has the following advantages when compared to spread spectrum modulation: higher data rate over a smaller bandwidth; more non-overlapping channels; increased resistance to reflected multipath signals; increased resistance to interference.

2.2.2.2 IEEE 802.11 WLAN Topologies

2.2.2.2.1 Infrastructure WLANs

The most common WLAN topology is the infrastructure mode where WLAN stations connect to the wired network through access points. *Figure 2-1, Enclave WLAN Architecture*, shows an example of an infrastructure mode WLAN.

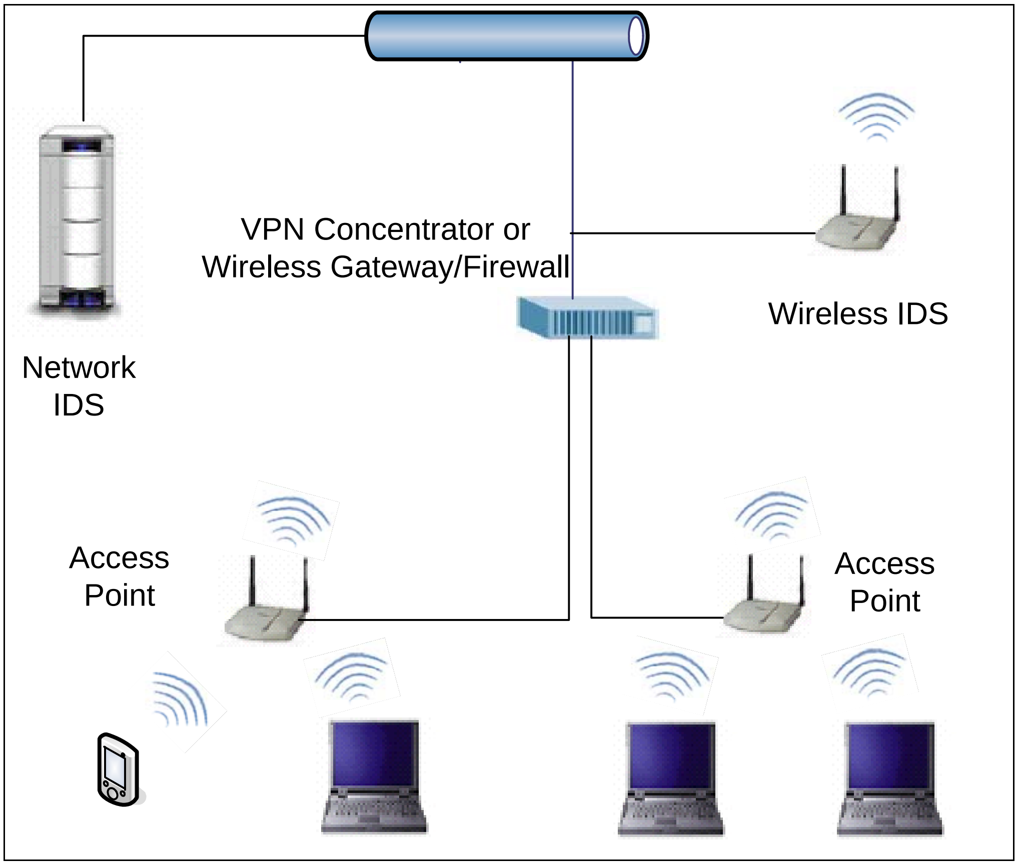


Figure 2-1. Enclave WLAN Architecture

2.2.2.2.2 Ad Hoc Wireless Networks

WLANs may be configured into a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly. This type of implementation can be as basic as two laptops with wireless NICs transmitting data back and forth where no access point is required. Peer-to-peer WLAN communications can bypass DOD required encryption and authentication mechanisms and, therefore, these transmissions are vulnerable and could be easily intercepted, providing unauthorized access to DOD data. To mitigate this risk, peer-to-peer WLAN networks may be used only with DAA approval and must comply with requirements in the following Sections: *Section 2.1, Introduction; Section 2.2.1.1, WLAN Stations/Clients; Section 2.2.4, Security Issues With Windows 2000, XP and Embedded Wireless Systems;* and *2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements*. Additionally, the following requirements apply:

- *(WIR0130: CAT II) The IAO will ensure WLAN Network Interface Cards (NICs) that do not have the capability to turn off or otherwise disable peer-to-peer WLAN communications are not used.*

- *(WIR0125: CAT II) The IAO will ensure strong mutual authentication between each station on the peer-to-peer network occurs before data is transmitted between stations.*

2.2.2.2.3 Wireless LAN Bridges

IEEE 802.11 WLAN systems can be used to provide a wireless communications link (or bridge) between two wired LANs, typically located in adjacent buildings. The hardware used in a wireless LAN bridge is similar to a wireless LAN access point, but instead of only connecting wireless clients to the wired network, bridges are primarily used to connect other wireless LAN bridges to the network.

NOTE: Most wireless LAN bridges can connect to both clients and other bridges. If a WLAN bridge is configured to allow connections to WLAN clients, the bridge should be configured IAW *Section 2.2.5* of this STIG.

- *(WIR0270: CAT II) The IAO will ensure FIPS 140-2 compliant encryption is used to secure the WLAN system (e.g., VPN or security gateway).*

NOTE: Either layer 2 or 3 security mechanisms with Triple Data Encryption Standard (3DES) or AES encryption are acceptable.

- *(WIR0290: CAT II) The IAO will ensure wireless access points and bridges are placed in a screened subnet (DMZ on firewall separating intranet and wireless network), or Virtual LAN (VLAN) and or otherwise separated from the wired internal network. A VPN concentrator or wireless security gateway/switch is placed between the bridge and the local DOD network.*

- *(WIR0072: CAT II) The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, Remote Access System (RAS), firewalls, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.*

- *(WIR0330: CAT I) The IAO will ensure management interfaces and management consoles for WLAN network devices are password protected and the password is compliant with DOD password policies.*

NOTE: WLAN network devices, communications devices, and management interfaces must be compliant with the requirements of the *Network Infrastructure STIG*.

2.2.3 802.11 Wireless LAN Security

In general, developing a wireless network security architecture is more complicated than developing a wired network security architecture. Limits on wireless device transmission bandwidth, processing power, data storage, and mobility require that, in most cases, different security mechanisms be used to provide user authentication and data encryption. For example, the Wireless Transport Layer Security (WTLS) protocol is used to encrypt data in many wireless networks instead of Secure Socket Layer (SSL). Additionally, most Wireless Internet Service Providers (WISPs) and wireless device manufacturers preset many of the security features of the network and client devices, thus the security manager may not be able to control all security aspects of the system. When designing and implementing a wireless network and wireless security architecture, the project manager and security manager must carefully evaluate the security requirements of the system against the security features of the wireless gateway, WISP, and wireless device.

Security mechanisms for a wireless network can generally be found at three locations in the International Standards Organization (ISO) Open Systems Interconnection (OSI) 7-layer model, which is depicted in *Figure 2-2, The OSI Model.*

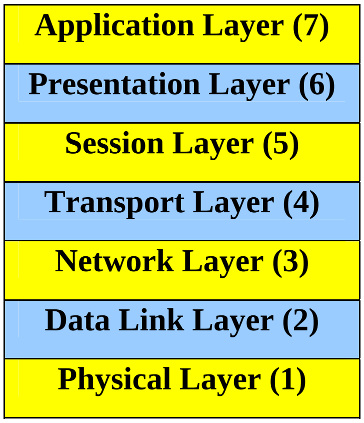


Figure 2-2. The OSI Model

At the Physical/Data Link layers many transmission protocols provide encryption and device identification. For WLANs, the Wired Equivalent Privacy (WEP) protocol, which is part of the IEEE 802.11 standard, and the Wi-Fi Protected Access (WPA) protocol provide these security services. For wireless PDAs, two-way e-mail devices, and cell phones, the radio/air interface protocol may provide these services between the wireless device and the wireless service provider base station.

At the Network/Transport layers, many wireless network providers provide secure Virtual Private Network (VPN) tunnels using standard protocols such as IP Security (IPSEC) or proprietary protocols. These secure tunnels encrypt all data between the wireless device and the wireless gateway (which may be located at the wireless service provider or on the government operated network) and may provide device identification and/or user authentication security services.

Security is also found at the presentation and application layers where user authentication and data encryption services are offered. End-to-end security is provided between the client application on the wireless device and the application server located in the government operated network. A number of standard and proprietary protocols are used to provide these security services including SSL and WTLS. In addition, several biometric security solutions are now available including fingerprint scanning and signature recognition. For a WLAN system, security services at the application layer are usually the same as those found in the wired part of the network.

Like all IEEE 802 standards, the 802.11 standards (802.11a, 802.11b, and 802.11g) focus on the bottom two layers of the OSI model—the physical and data link layers. Security mechanisms of the 802.11 standard, such as access control and encryption, operate at the data link layer, particularly the MAC sublayer. The 802.11 MAC sublayer can work seamlessly with standard Ethernet, via a bridge or access point, to provide a connection between wireline and wireless nodes. For this reason, once the access point is reached, the same security standards supported by other 802-compliant LANs for access control (such as network operating system logins) and encryption (such as IPSec or application-level encryption) apply.

Wired Equivalent Privacy (WEP) Protocol, the original IEEE 802.11 security protocol, was found to have a number of significant security vulnerabilities. Over the past three years the IEEE and the Wi-Fi Alliance industry group have released two new security protocols to improve WLAN security and interoperability. Wi-Fi Protected Access (WPA) was the first new WiFi security protocol. WPA fixed a number of the known security problems with WEP but a number of security vulnerabilities remained. In early 2004 the WiFi Alliance released WPA2, which is based on the IEEE 802.11i security specification. A number of WPA2 (also called RSN) certified products became available in late 2004 but these products are not necessarily approved for use in DOD. Consult the NIST FIPS 140-2 Validated Products List prior to procuring WPA2 certified products to determine if the specific product is also FIPS 140-2 certified.

2.2.3.1 Service Set Identifier (SSID)

Although advertised as a means of simple access control for an access point or group of access points, the SSID should not be considered a safe or reliable access control mechanism. The SSID is an alphanumeric code that corresponds to a specific wireless network (or subsystem). Usually, in the default configuration of an access point, the SSID is transmitted in the clear as a part of a periodic beacon that is sent by the access point or it may be requested in a probe-request frame when a wireless client attempts to associate with an access point with a specific SSID. Most access points permit the broadcast of their identifier so that wireless stations within range know that the access point is available for a client to connect to it. Good security practice dictates that an access point should not advertise its presence and should only respond to clients that know its SSID.

- *(WIR0140: CAT III) The IAO will ensure SSIDs are changed from the manufacturer's default to a pseudo random word consisting of a combination of upper and lower case characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure the SSID broadcast mode is disabled and that WLANs that do not allow the SSID broadcast mode to be disabled and are not used.*

2.2.3.2 MAC Address Filtering

Just as an access point or group of access points can be identified by the SSID, a client in a WLAN can be identified by the unique MAC address of its 802.11 wireless NIC. Therefore, another type of access control can be implemented based on permitting access to only those MAC addresses that are known to belong to legitimate users. Only devices having MAC addresses matching those on the list are permitted access to the WLAN. MAC related information in the header of a datagram is sent in the clear so it is possible that the MAC address can be obtained by eavesdropper and spoofed in an attempt to gain access to the WLAN. Although MAC address filtering provides only minimal security, it should be implemented as a deterrent to the casual hacker.

- *(WIR0160: CAT III) The IAO will ensure MAC address filtering is enabled at each access point.*

NOTE: MAC address filtering may not be practical for large WLAN implementations, unless the WLAN management system allows for MAC distribution lists to be centralized and automatically distributed to the point of authentication.

2.2.3.3 WEP Protocol

Although it has been replaced by the IEEE 802.11i specification, WEP is still used by many WLAN installations. WEP is the original security specification for the 802.11 standard. There are two types of authentication/access control defined by the WEP protocol—open system authentication and shared key authentication. With open system authentication, the access point grants access to stations with an authorized SSID. With shared key authentication, both the access point and any station authorized to connect to the access point share a key that is used for both authentication and encryption.

Most WLAN products with WEP offer both 64-bit and 128-bit WEP encryption. The WEP encryption key is comprised of a shared key and a 24-bit initialization vector (IV). The 64-bit WEP key is formed by combining a 40-bit shared key and the IV. The 128-bit WEP key is formed by combining a 104-bit shared key and the IV. Some WLAN products allow the IV to be changed periodically, including as often as after every transmission.

Unfortunately, the WEP protocol is a flawed application of cryptographic principles and design. Some known attacks exploit problems with both the encryption and authentication provided by WEP. These flaws occur because the WEP standard uses static, reusable shared secret keys and a poor implementation of the RC4 algorithm. In addition, the IV is transmitted in clear text and is usually changed in a predictable pattern. Several studies have concluded that with minimal hardware/software and statistical analysis (intercepting a minimal amount of wireless traffic), WEP keys can be easily determined. Then with these keys exploited (shared secret key and IV), an unauthorized individual can determine the encryption key and gain access to the data being transmitted and, potentially, to all connected backend resources.

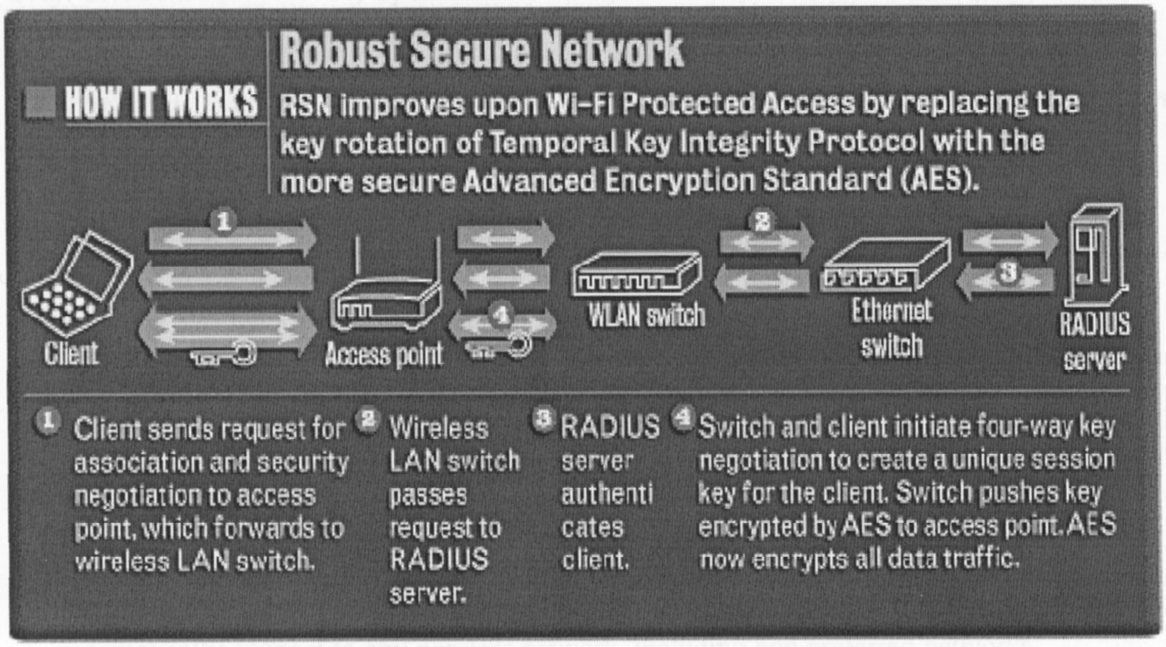
NOTE: WEP security may be enabled and used as part of a defense-in-depth approach on DOD wireless systems.

2.2.3.4 Wi-Fi, WPA, and WPA2

The Wi-Fi Alliance industry group certifies WLAN products as meeting specific standards. When a WLAN product is marked as Wi-Fi compliant, the product was evaluated by the Wi-Fi Alliance laboratory and meets the requirements found in the IEEE 802.11a, b, or g standards. The product may also be evaluated as WPA or WPA2 compliant. Note that WPA or WPA2 compliant products must be separately evaluated by NIST to determine if they are FIPS 140-2 compliant.

WPA was based on a draft (pre-release) version of the IEEE 802.11i security specification. Unlike WEP, WPA does not use fixed encryption keys, but instead uses a network password that initiates a key rotation every 10,000 bytes of data using the 802.11i's Temporal Key Integrity Protocol (TKIP). Since WPA uses the same RC4 encryption algorithm found in WEP, Wi-Fi certified WLAN products with WPA do not meet DOD security policies.

Products certified as Wi-Fi WPA2 implement the requirements of the IEEE 802.11i specification, which uses a number of authentication and security protocols to establish secure wireless communications. RSN is used to establish a secure wireless connection between wireless devices. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and stations. The authentication schemes are based on IEEE 802.1x and EAP with Advanced Encryption Standard (AES) as the encryption algorithm. Dynamic negotiation of the authentication and encryption algorithms allows the use of new algorithms as they are developed. *Figure 2-3, Robust Secure Network,* details the steps of the RSN protocol.



RSN improves upon Wi-Fi Protected Access by replacing the key rotation of Temporal Key Integrity Protocol with the more secure Advanced Encryption Standard (AES).

1 Client sends request for association and security negotiation to access point, which forwards to wireless LAN switch.

2 Wireless LAN switch passes request to RADIUS server.

3 RADIUS server authenticates client.

4 Switch and client initiate four-way key negotiation to create a unique session key for the client. Switch pushes key encrypted by AES to access point. AES now encrypts all data traffic.

Figure 2-3. Robust Secure Network

Wireless Robust Authentication Protocol (WRAP) is an optional component of RSN that uses the Offset Codebook (OCB) mode of AES to encrypt data. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is the preferred encryption protocol in the IEEE 802.1i specification.

2.2.3.5 SecNet 11

The Secure Wireless LAN (SWLAN) solution developed by Harris Corporation provides transparent, NSA Type-1 certified encrypted data communications using the SecNet 11 products in a WLAN environment. The SecNet 11 wireless NIC uses a Harris Sierra™ Encryption Module, Intersil PRISM™ II chipset, and Baton encryption algorithm. The card operates in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band using a modified IEEE 802.11b protocol, which takes into account crypto delays. The cryptographic function is embedded in the card. SecNet 11 users can send and receive secure data, voice, and video between and among equipped wireless stations. The SecNet 11 is certified for processing data classified up to DOD Secret.

The SecNet 11 only provides data encryption; it does not have any user identification or authentication capabilities. Therefore, when the SecNet 11 is used to secure a wireless LAN, additional identification and assurance equipment is needed to meet the security requirements of *DODD 8100.2*.

NSA distributes both classified and unclassified operational keys for the SecNet 11 WLAN; therefore, SecNet 11 is available for unclassified WLANs that process highly sensitive information. COMSEC accounts are required for organizations that plan to use the SecNet 11.

The *Secure Wireless Local Area Network Addendum to the Wireless STIG* contains detailed guidance on procedures for obtaining required approvals for connecting a SWLAN to the SIPRNet and should be reviewed before implementing a SecNet 11 WLAN.

Harris Corporation has also developed an NSA Type-1 certified WLAN product called the SecNet 54, which will provide a WLAN based on the IEEE 802.11 a, b, or g standards (depending on which radio adapter is used). Approval for the use of the SecNet 54 in SWLAN implementations is expected very shortly. This product will be certified to process classified information up to Top Secret.

- *(WIR0200: CAT III) The IAO will ensure the CTTA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data.*

- *(WIR0204: CAT I) The IAO will ensure before a SWLAN becomes operational and is connected to the SIPRNet the following occurs:*

- *The SWLAN system is certified and accredited by the DITSCAP process.*

- *A SIPRNet connection approval package is submitted to the SIPRNet Connection Approval Office (SCAO).*

- *The DSAWG has approved the connection.*

- *(WIR0041: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

- *(WIR206: CAT III) The IAO will ensure written operating procedures exist that describe procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material in a SWLAN operational environment.*

2.2.4 Security Issues With Windows 2000, XP and Embedded Wireless Systems

Windows XP (and updated Windows 2000) has inherent wireless support features, provided by the Wireless Zero Configuration (WZC) service. The WZC service has a number of security vulnerabilities:

- The Automatic Network Detection and Association feature, which is enabled by default in Windows XP (pre XP SP1), causes the computer to automatically detect and attempt to associate (connect) to any wireless device that can be "seen" by the wireless NIC in the computer. The WZC service will attempt to automatically connect to wireless networks based on the networks listed in the "Preferred Networks" list. This default setting can be changed to allow the WZC service to automatically connect to any wireless network, including non-preferred networks.

- Windows 2000 and XP will "leak" SSID information on any registered and approved SSID to which it has been previously connected. A list of all the access points to which the computer has ever connected is stored in XP. Upon boot-up or when out of access point range, the computer continually transmits queries, attempting to reconnect to an access point. These queries contain the SSID of all access points to which the computer has previously connected. A hacker can easily sniff the content of these queries, obtain the embedded SSIDs, and use the information to program a rogue access point. (This is an example of why SSIDs should not be considered a good security mechanism.)

- When a third party PEAP utility is used for authentication, each 802.11-associated update to Windows XP may overwrite the PEAP settings. In most cases, the PEAP utility will have to be reinstalled.

- Windows XP SP2 provides the capability to disable WZC service from automatically connecting to wireless systems on the "Preferred Networks" list. This capability is not available with Windows 2000.

Security requirements for Windows 2000 and XP (pre SP2) wireless systems are as follows:

- *(WIR0163: CAT III) The IAO will ensure the WZC service is disabled in any Windows 2000 and XP computer that is used on a wireless LAN. This setting should be verified whenever new software or operating system updates are installed on the computer.*

- *(WIR0164: CAT III) The IAO will ensure only WLAN drivers and WLAN management software from third party sources that do not depend on the WZC service are used in Windows 2000 and XP computers. (Check with WLAN vendor prior to purchasing equipment.)*

NOTE: The WZC service may not be used to manage WLAN connections to the computer. Instead, the WLAN software that is usually provided by the WLAN interface card vendor should be installed and used.

- *(WIR0165: CAT III) The IAO will ensure WLAN users with Windows XP computers remove the WLAN NIC whenever wireless service is not being used.*

Security requirements for Windows XP (SP2) wireless systems are as follows:

- *(WIR0168: CAT III) The IAO will ensure the WZC service "Preferred Network" connection is configured on Windows XP SP2 computers as follows: the "Connect when this network is in range" selection are disabled on the Connection tab.*

- *(WIR0165: CAT III) The IAO will ensure WLAN users with Windows XP computers remove the WLAN NIC whenever wireless service is not being used.*

Laptop computers with embedded wireless LAN cards (mini PCI cards) are particularly susceptible to the Windows XP wireless vulnerabilities described above. Most laptop vendors provide a software utility to manage WLAN connections for the embedded wireless cards. The utility usually provides a feature that allows a laptop user to turn off the WLAN card radio. The default setting of all embedded WLAN card radios should be set to the "*OFF*" setting.

- *(WIR0166: CAT III) The IAO will ensure Windows XP computers with embedded wireless LAN cards are purchased after the following is verified:*

- *The installed WLAN interface card can be operated with the Windows XP WZC service disabled.*

- *The laptop vendor provides a WLAN card management utility.*

- *The WLAN card management utility has the capability to turn off the radio of the embedded WLAN card.*

- *(WIR0167: CAT III) The IAO will ensure laptops with embedded WLAN cards have the WLAN card radio set to OFF as the default setting.*

2.2.5 IEEE 802.11 WLAN Implementation Compliance Requirements

The compliance requirements in this section apply to WLAN access points, bridges (that allow wireless client connections), stations (clients), gateways and switches.

- *(WIR0070: CAT III) The IAO will ensure WLAN devices installed outside the Continental United States (CONUS) have been approved by the local U.S. Forces Command (USFORSCOM) and/or host nation.*

2.2.5.1 Classified WLAN Systems

The DAA has the responsibility to ensure that only NSA Type-1 certified WLAN systems are used for the wireless transmission of classified information. All wireless systems must receive the approval of the Defense Security Accreditation Working Group (DSAWG) prior to connecting them to the SIPRNet.

- *(WIR0170: CAT II) The IAO will ensure WLANs are used to store, process, or transmit classified and/or SCI information only up to the classification level the system has been approved by NSA to support.*

NOTE: For example, Secret and below for SecNet 11 and Top Secret, and below for SecNet 54.

- *(WIR0180: CAT II) The IAO will ensure WLAN devices (for all classification/sensitivity level of information) are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) unless approved by Director Central Intelligence Directive (DCID) 6/9 or 6/3.*

- *(WIR0190: CAT II) The IAO will ensure computers with embedded WLAN systems that cannot be removed by the user are not used to store, process, or transmit classified information.*

- *(WIR0070: CAT III) The IAO will ensure WLAN devices installed outside of CONUS have been approved by the local USFORSCOM and/or host nation.*

- *(WIR0009: CAT I) The IAO will ensure all classified wireless systems are approved by the DAA prior to installation and use for processing classified DOD information.*

- *(WIR0200: CAT III) The IAO will ensure the CTTA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data.*

- *(WIR0203: CAT I) The IAO will ensure only NSA Type-1 certified WLAN systems are used for wireless transmission of classified information.*

- *(WIR0210: CAT II) The IAO will ensure WLANs approved for processing classified information use DOD PKI certificates for user authentication.*

NOTE: *SecNet 11 does not provide user identification and authentication.*

- *(WIR0220: CAT II) The IAO will ensure tools are used to encrypt classified data at rest on the wireless device. Encryption tools must be NSA Type-1 certified.*

NOTE: Currently there are no NSA Type-1 certified encryption tools for Personal Digital Assistants (PDA).

- *(WIR0225: CAT II) The IAO will ensure WLANs are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

- *Approved by the DAA in consultation with the CTTA.*

- *The WLAN equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *(WIR0204: CAT I) The IAO will ensure before a SWLAN become operational and is connected to the SIPRNet the following occurs:*

- *The SWLAN system is certified and accredited by the DITSCAP process.*

- *A SIPRNet connection approval package is submitted to the SIPRNet Connection Approval Office (SCAO).*

- *The DSAWG has approved the connection.*

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

- *(WIR0205: CAT II) The IAO will ensure access points and clients for wireless devices processing classified data, including the SecNet 11, are physically secured to prevent tampering/reprogramming (prevent unauthorized physical access).*

- *(WIR0206: CAT III) The IAO will ensure written operating procedures exist that describe procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material in a SWLAN operational environment.*

-

2.2.5.2 Unclassified WLAN Systems

With DAA approval, 802.11a, 802.11b, and 802.11g solutions will be used for unclassified data provided all of the following conditions are met:

- *(WIR0140: CAT III) The IAO will ensure SSIDs are changed from the manufacturer's default to a pseudo random word consisting of a combination of upper and lower case characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure the SSID broadcast mode is disabled and WLANs that do not allow the SSID broadcast mode to be disabled will not be used.*

- *(WIR0160: CAT III) The IAO will ensure MAC address filtering is turned on at each access point.*
- *(WIR0230: CAT II) The IAO will ensure the wireless LAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy.*

- *(WIR0240: CAT II) The IAO will ensure PKI certificates are used for identification and authentication (I&A) of the user.*

- *(WIR0250: CAT II) The IAO will ensure the WLAN access point is set to the lowest possible transmit power setting, which meets the required signal strength of the area serviced by the access point.*

- *(WIR0260: CAT II) The IAO will ensure all data at rest is encrypted on all WLAN client devices. Encryption system must be FIPS 140-2 certified.*

- *(WIR0270: CAT II) The IAO will ensure FIPS 140-2 compliant encryption is used to secure the WLAN system (e.g., VPN or security gateway).*

NOTE: Either layer 2 or 3 security mechanisms with 3DES or AES encryption are acceptable.

- *(WIR0280: CAT II) The IAO will ensure if a wireless LAN device is to be used to access a DOD network via the Internet through a public WLAN/Internet gateway (e.g., airport or hotel "hotspot"), the following requirements are met:*

- *When using a PDA for remote access, the PDA compliance requirements in the Wireless STIG are followed.*

- *The requirements in the Secure Remote Computing STIG are followed.*

- *(WIR0075: CAT III) The IAO will ensure the organization periodically screens for unauthorized or rogue access points, stations, and bridges. Local security policy will address the frequency for which these screenings should occur.*

The IAO will ensure that access points are protected from attack as follows:

- *(WIR0290: CAT II) The IAO will ensure wireless access points and bridges are placed in a screened subnet (DMZ on firewall separating intranet and wireless network), or Virtual LAN (VLAN) and or otherwise separated from the wired internal network. A VPN concentrator or wireless security gateway/switch is placed between the access point and the local DOD network.*

- *(WIR0300: CAT II) The IAO will ensure a wired or wireless IDS or Intrusion Prevention System (IPS) is used to monitor the wireless network.*

It is strongly recommended that both wired and wireless IDS/IPS be used to continuously monitor approved wireless networks and search for unapproved "rogue" wireless networks at all DOD sites with WLAN systems.

- *(WIR0072: CAT II) The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, Remote Access System (RAS), firewalls, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.*

- *(WIR0330: CAT I) The IAO will ensure WLAN network device management interfaces and management consoles are password protected and the password is compliant with DOD password policies.*

The IAO will ensure that client stations are protected as follows:

- *(WIR0100: CAT III) The IAO will ensure a personal firewall is implemented on each 802.11-enabled wireless device to block unauthorized access to the device and the software is configured in accordance with the* Desktop Application STIG.

- *(WIR0090: CAT III) The IAO will ensure an access control mechanism is placed on all 802.11-enabled devices.*

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

- *(WIR0460: CAT II) The IAO will ensure tools are used to encrypt data at rest on the wireless device. Encryption tools must be FIPS 140-2 certified.*

- *(WIR0161: CAT II) The IAO will ensure computer/PED wired network interfaces (e.g., Ethernet) are disconnected or otherwise disabled when wireless network connections are being used.*

WLAN stations (e.g., PCs, laptops, PDAs) should only be purchased after it has been verified that a personal firewall, antivirus software, and file encryption software are available for that equipment.

2.2.6 WLAN Common Criteria Protection Profiles

NSA is developing a suite of protection profiles (PP) focused on wireless networking technologies. For WLANs, the first PPs, the *U.S. Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments Protection Profile* and *U.S. Government Wireless Local Area Network (WLAN) Client for Basic Robustness*, focuses on IEEE 802.11a/b wireless LAN access devices. (All PPs can be found at www.nist.gov/cc-scheme/cc_docs/.) The PPs specify the minimum-security requirements for a WLAN Access System and Client used by the U.S. Government in basic robustness environments. NSA is also currently developing WLAN Access System and Client PPs for medium robustness environments. The assurance requirements specified in the Medium robustness PP will be Evaluation Assurance Level (EAL) 4. The assurance specified in the Basic robustness PP is EAL 2. The target robustness level of "basic" and "medium" are specified in DOD Instruction 8500.2.

This PP discusses a typical wired to wireless configuration. However, the PP does not preclude any other wireless configuration that may exist. This wireless access system may vary in the type of components used to provide access to the wired LAN. This PP does not dictate a particular configuration. Instead the PP addresses the security requirements for the system that allows access to the wired network while performing management functions within the system. The security requirements of the Target of Evaluation (TOE) are identification and authentication (I&A), audit, encryption, information flow control, and administration. This PP requires privacy and integrity of communications over a WLAN, using commercially available cryptographic algorithms. The assurance requirements specified in the PP are EAL 2 augmented with flaw remediation, assurance maintenance and misuse analysis.

The *Wireless LAN Access System Protection Profile* received approval from the NSA PP Review Board (PPRB) and has been submitted to the National Information Assurance Partnership (NIAP). Once it is submitted to a lab for evaluation, the WLAN Access System PP will be available as the official U.S. Government security requirements for wireless access systems used on U.S. Government systems at the Basic robustness level. The final draft for the WLAN client PP is currently undergoing evaluation by a Common Criteria lab and will be available as the official U.S. Government security requirements for WLAN clients used on Government systems.

2.3 Bluetooth WPAN

The Bluetooth Special Interest Group (SIG), which is a group of companies interested in promoting Bluetooth wireless solutions, developed the Bluetooth specification. IEEE 802.15 WPANs formalizes the specification. The primary goal of the specification is to define wireless connectivity for fixed, portable, and moving devices within or entering a POS of the user. The goal is to achieve interoperability (e.g., no radio interference) between a WPAN device and any IEEE 802.11 WLAN device. Interference between WLAN technology and Bluetooth (IEEE 802.15 WPAN) networks can be a significant problem, as they both operate in the same frequency band. The IEEE 802.15 Task Group 2 (TG2) is developing coexistence mechanisms for the two standards. The IEEE 802.15.1 standard defines device-level authentication at the data link layer and data encryption at the physical layer.

Bluetooth enabled electronic devices connect and communicate wirelessly via short-range (100m or less) in ad hoc networks called piconets. Bluetooth and 802.11 wireless technologies share some characteristics and overlap slightly in some usage models, but they serve fundamentally different purposes.

Bluetooth systems can be operated in the DOD, provided they meet the security compliance requirements listed in *Section 2.3.1 Bluetooth Compliance Requirements*. Security for a Bluetooth network can be found at both the physical and data link layers of the protocol. Bluetooth uses FHSS modulation that provides a 1600 hops/sec frequency-hopping rate and, along with low output transmission power and short transmission range and provides a formidable barrier to anyone trying to eavesdrop on a connection (see *Table 2-1*).

Device Class	Strength	Range (Meters)
Class 1	100 mW	Up to 100
Class 2	2.5 mW	Up to 10
Class 3	1 mW	About 1

Table 2-1. Bluetooth Power and Range Specifications

At the data link layer, Bluetooth provides both authentication and encryption. Each Bluetooth device has a unique device address that is used to authenticate the devices. Either one-way, two-way, or no authentication may be specified. For encryption, Bluetooth uses an algorithm where the key length is selectable between 8 and 128 bits. This allows Bluetooth to be used in countries that limit the length of encryption keys. The encryption key size in a specific Bluetooth device must be set at the factory in order to prohibit the user from overriding the permitted key size.

Bluetooth has many of the same security management problems found with the IEEE 802.11b standard (pre-802.11i release) in that no process is defined for managing the process for issuing, validating, and revoking link keys. Bluetooth provides for built-in encryption and authentication, but like 802.11b, additional security products must be used to mitigate this standard’s inherent security shortcomings. There were no Bluetooth specific FIPS 140-2 security products available at the time this document was released.

Additional information on Bluetooth security issues can be found in NSA IA Advisory IAA 004-2004, Vulnerabilities and Countermeasures Associated with Integrated Bluetooth capability, 13 May 2004.

In addition to Bluetooth, there are several other PAN system standards defined by the IEEE 802.15 working group. The four IEEE 802.15 standards are as follows:

- IEEE 802.15.1 Bluetooth

- IEEE 802.15.2 Coexistence. Standard that defines the coexistence between WPAN and WLAN systems.

- IEEE 802.15.3 WPAN high rate standard, WiMedia (>= 20Mbps)

- IEEE 802.15.3a WPAN ultra high rate standard, Ultra Wideband (UWB), (>= 110 Mbps)

- IEEE 802.15.4 WPAN low rate, Zigbee (20-250 Kbps). Used for sensors, interactive toys, and home automation.

2.3.1 Bluetooth Compliance Requirements

2.3.1.1 Classified Information

- *(WIR0009: CAT I) The IAO will ensure all wireless systems are approved by the DAA prior to installation and use for processing classified DOD information.*

- *(WIR0182: CAT I) The IAO will ensure Bluetooth devices are not used to send, receive, store, or process classified messages.*

- *(WIR0181: CAT I) The IAO will ensure Bluetooth devices are not permitted in a permanent, temporary, or mobile SCIF unless approved by Director Central Intelligence Directive (DCID) 6/9 or 6/3 and the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0225: CAT I) The IAO will ensure Bluetooth devices are, if allowed, operated in areas where classified discussions or data processing takes place only when:*

- *The DAA, in consultation with the CTTA, has approved the use of Bluetooth devices and they can be brought into the facility and/or used in the facility.*

- *The device's voice recording capability is rendered inoperable.*

- *The Bluetooth devices are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.*

2.3.1.2 Unclassified Information

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0080: CAT II) The IAO will ensure Bluetooth devices are not used to store, process, or transmit DOD information, unless FIPS 140-2 validated cryptographic modules are used to encrypt the data during transmission.*

- *(WIR0083: CAT III) The IAO will ensure the Bluetooth capability is removed or disabled from the wireless device if FIPS 140-2 validated cryptographic modules are not used.*

2.4 Wireless Mice and Keyboards

Wireless keyboard and mice are increasingly used throughout DOD. These devices use various wireless technologies such as WLAN, Bluetooth, and IR to transmit data to the computer. Wireless mice transmit telemetry data (right, left, etc.), while wireless keyboards transmit users' keystrokes.

The following conditions will be met prior to the use of wireless mice or keyboards:

- *(WIR0132: CAT II) The IAO will ensure if WLAN or Bluetooth mice and keyboards are used, applicable requirements listed in Section 2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements, or Section 2.3, Bluetooth WPAN, are followed.*

- *(WIR0131: CAT II) The IAO will ensure if infrared wireless mice and keyboards are used on classified or unclassified equipment and networks, the following conditions are followed:*

- *The DAA, in consultation with the CTTA, has approved IR wireless mice and/or keyboards for use in the facility.*

- *When wireless mice and/or keyboards are used on classified equipment, the area is approved for processing classified information at the appropriate level.*

- *The area is totally enclosed with walls, ceiling, and floor consisting of material opaque to IR. There are no windows unless each window is covered with a film approved for blocking IR. All doors must remain closed when the devices are in operation.*

- *There is no mixing of classified and unclassified equipment using IR within the same enclosed area.*

- *When IR is used with classified equipment in the same enclosed area as unclassified equipment with IR ports, the IR ports on the unclassified equipment must be completely covered with metallic tape.*

- *When IR is used with unclassified equipment in the same enclosed area as classified equipment with IR ports, the IR ports on the classified equipment must be completely covered with metallic tape.*

2.5 Voice Over IP (VoIP) WLAN Systems

Wireless VoIP systems offer the convenience of a mobile or cellular phone combined with the cost savings of a VoIP telephone system.

The following conditions will be met prior to the use of wireless VoIP systems:

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0133: CAT II) The IAO will ensure all wireless VoIP systems comply with applicable requirements in the Wireless STIG, Section 2.2.5, IEEE 802.11 WLAN Implementation Compliance Requirements,* and the *VoIP STIG.*

2.6 WWAN Technologies, Protocols, and Security

2.6.1 Introduction

Commercial WWAN data services (also called wireless broadband) began to be used in the U.S. in the early 1990s as low speed (less then 30 Kbps) data networks and were used primarily for pagers, wireless PDAs, and email devices (e.g., Blackberry). In the late 1990s wireless data broadband services (100 Kbps – 1+ Mbps) started to become available. The development and subsequent deployment of WWAN services has followed two paths: cellular based standards (3G services) and IEEE standards based services. This section discusses both legacy wireless data services and IEEE standards based WWAN services. Cellular based wireless data services are reviewed in *Section 3.2.1, Wireless Telephone Protocols*.

2.6.2 Legacy PDA Wireless Air Interface Protocols

This section describes the two most prevalent low speed radio interface protocols that have been used in the United States for PDA and laptop wireless Internet access. Wireless carriers started discontinuing these services in 2004.

- Cellular Digital Packet Data (CDPD) is an open standard for packet data service that is integrated with existing AMPS and IS-136 TDMA networks. CDPD provides data rates up to 19.2 Kbps and is one of the primary data protocols for wireless PDA services. CDPD provides device-level authentication and data encryption between the wireless device and the carrier base station. In addition, the standard includes sophisticated anti-cloning protection. Cingular, Verizon, and GoAmerica provide CDPD services.

- Mobitex is an open standard for a narrow band data packet switching network that is used by several wireless PDAs and older BlackBerry e-mail devices. Cingular, Verizon and Velocita operate national Mobitex networks in the US. Mobitex security primarily consists of device-level authentication using an embedded device ID number, but this number is subject to the same cloning problems as analog cellular phones. Although the standard includes data bit scrambling, this is done for technical reasons and should not be considered data encryption. Most wireless PDA service providers, including Palm.net, provide secure application level data encryption services.

2.6.3 IEEE 802.16 BWA Technology

The IEEE 802.16 (BWA) standard (also known as Wi-MAX) defines interoperability requirements for Wireless Metropolitan Area Networks (WMANs) that operate in the 2 – 66 GHz frequency range. These networks offer subscriber local loop service (similar to a local telephone service) and wireless hotspots for Internet connections (similar to an 802.11b WLAN hot-spot) and compete with both public 802.11 and broadband 3G cellular services. BWA networks focus on the first mile/last mile connection in WMAN networks and provide broadband alternatives to DSL, cable, or T-1 services. Data rates for BWA systems vary and depend on the specific implementation but subscribers should expect data rates equal to or greater than T-1 and DSL (1.5 Mbps+).

BWA systems are usually deployed in a Point to Multipoint (PMP) topology where the base station services multiple subscribers located in the broadcast area of the base station. The base station is collocated with an entry point of the service provider’s backhaul system and connects to the Internet backbone through the backhaul system. The BWA standard defines an optional topology, called Mesh Mode, for areas of high user density or areas were subscribers do not have line of sight to a base station located at the backhaul system entry point (airhead). In a mesh network, intermediate base stations (intermediate devices) have the capability to route traffic to other intermediate devices until the airhead is reached. Mesh networks are designed so that there are multiple paths between each intermediate device and the airhead, thus providing system redundancy.

WMANs are beginning limited deployment in the United States. In general, WMAN systems do not include security services. Therefore, DOD WMAN subscribers should assume that the WMAN system does not meet DOD security requirements and that additional security measures (e.g., VPN) are required before using these systems.

2.6.4 IEEE 802.20 Mobile Broadband Wireless Access (MBWA) Technology

The emerging MBWA specification is designed to address performance gaps between high data-rate low mobility services of WLAN and WMAN systems and high mobility cellular networks. The goals of the specification are to provide user data rates in excess of 1Mbps, support mobile users in vehicles traveling up to 250 Km/h (150 miles/h), and operate in frequency bands below 3.5GHz. MBWA systems are expected to compete directly with cellular 3G broadband services. Deployment of MBWA systems is not expected until at least 2006.

2.6.5 Broadband Wireless System Compliance Requirements

2.6.5.1 Classified Broadband Wireless Systems

Currently there are no NSA approved commercial WWAN wireless devices for storing, processing, or transmitting classified and/or SCI information.

- *(WIR0373: CAT I) The IAO will ensure WWAN systems are not used to store, process, or transmit classified and/or SCI information.*

- *(WIR0374: CAT I) The IAO will ensure WWAN devices are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF).*

- *(WIR0375: CAT I) The IAO will ensure WWAN systems are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

- *Approved by the DAA in consultation with the CTTA.*

- *The WWAN system is operated in an area where classified information is electronically stored, processed, or transmitted, the broadband wireless system equipment is separated from the classified data equipment the distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, is implemented.*

2.6.5.2 Unclassified WWAN Systems

WWAN system solutions can be used for unclassified data provided all of the following conditions are met:

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0376: CAT II) The IAO will ensure DOD PKI certificates are used for I&A of the user.*

- *(WIR0377: CAT II) The IAO will ensure a FIPS 140-2 compliant VPN or security gateway/firewall is used to secure the WWAN system.*

NOTE: Either layer 2 or 3 security mechanisms with 3DES or AES encryption are acceptable.

- *(WIR0378: CAT III) The IAO will ensure the requirements in the Secure Remote Computing STIG are met.*

The IAO will ensure client stations are protected as follows:

- *(WIR0100: CAT III) The IAO will ensure a personal firewall is implemented on each 802.11-enabled wireless device to block unauthorized access to the device and the software is configured in accordance with the* Desktop Application STIG.

WWAN client equipment (e.g., PCs, laptops, PDAs) should only be purchased after it is verified that a personal firewall is available for that equipment.

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

2.7 RFID Technologies

RFID Technologies are increasingly used throughout the Federal Government, primarily to facilitate inventory control of equipment, track the contents of shipping containers, or to facilitate logical access to computer systems. The DOD has been a leader in implementing RFID systems in the Federal Government.

There are two main types of RFID systems: passive and active. Passive systems store data in a small electronic device (tag) that contains electronic memory and a low power radio transmitter/receiver. The tag has no internal power. The passive tag converts radio signals received from a reader, which is placed within 12 feet. These signals are converted into electrical power and used to transmit the data stored on the tag to the RFID reader. By contrast, active systems contain a battery and transmit stored information when queried by an RFID reader. Active systems can be designed to transmit data at distances from a few inches to a few hundred feet.

RFID transmissions can be intercepted by any receiver located within the transmit range of an RFID tag and operating on the same frequency as the tag. A RFID tag can be designed to require that the tag receive a valid passcode before stored information is transmitted. Note that reader authentication is rarely found in passive RFID systems. Since data encryption is not used with RFID systems, passcodes transmitted to RFID tags by RFID receivers are vulnerable to interception and reuse by nearby hackers.

RFID tags can contain any stored data, including user IDs and passwords. RFID tags can be designed so that the information stored on the tag cannot be modified or can be modified only by specific RFID readers, thus ensuring data integrity. Information stored on active and passive RFID tags is generally always available. Information stored on active RFID tags would not be available if the tag battery was fully discharged.

DODD 8100.2 specifically excludes RFID devices from being covered by the wireless security requirements listed in the directive. DOD agencies should conduct a risk assessment before using RFID devices to store sensitive information.

3. WIRELESS PED TECHNOLOGIES

3.1 Introduction

The use of PEDs, including cell phones, 2-way pagers, PDAs, laptops, and wireless email devices, is widespread in the DOD. Various wireless technologies are in use, including cellular, broadband cellular (3G), broadband wireless, and WLANs, that provide wireless network connectivity for PEDs. The convergence of mobile phone, PDA, and wireless email into one device has made it more difficult to determine the security requirements of these devices when used in the DOD environment.

This section will focus on cellular devices (including Short Messaging Service (SMS), Multimedia Messaging Service (MMS), and 2-way paging service), PDAs, and Blackberry wireless email devices that use these wireless technologies to connect to the Internet and DOD networks.

3.2 Cellular Technologies, Protocols, and Security

3.2.1 Wireless Telephone Protocols

This section provides an overview of radio interface standards and protocols used by wireless carriers in the United States.

Analog wireless communications protocols, in general, provide no security services. Analog cellular calls can be easily intercepted and the Mobile Identification Number (MIN) and Electronic Serial Number (ESN) can then be extracted from the intercepted call. Analog wireless phones can be easily cloned using intercepted MINs and ESNs. However, nearly all analog wireless carries have added device-level authentication, which is cross-referenced to the MIN and ESN, and ensures that a wireless phone is registered with the network before a call will be connected. Voice encryption services are not provided.

All digital wireless carrier systems provide device level authentication and data encryption. Some networks, such as Global System for Mobile communications (GSM), also provide user authentication.

3.2.1.1 1st Generation (1G) Technologies (Analog)

The Advanced Mobile Phone Service (AMPS) has been the American analog cellular standard since the 1970s. Developed by AT&T, this standard uses Frequency Division Multiple Access (FDMA) whereby the assigned radio spectrum is divided into channels and each channel is used for either the receive or the transmit portions of the wireless phone call. See *Figure 3-1, Wireless Radio Interface Protocols*. One of the shortcomings of AMPS is the lack of inherent security features (authentication and data encryption) in the standard.

Currently, the FCC requires all U.S. cellular carriers to provide analog cellular services. In August 2002 the FCC ruled that U.S. cellular carriers could begin to phase out analog cellular services in five years.

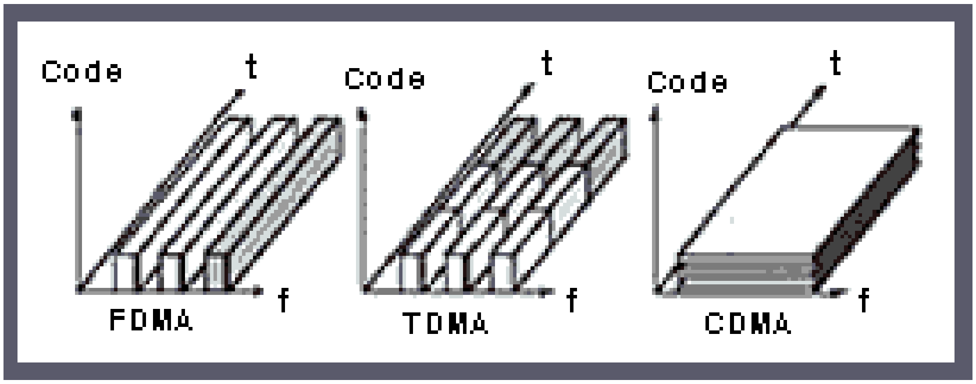


Figure 3-1. Wireless Radio Interface Protocols

- *Code division multiple access (CDMA).* TIA IS-95, published by the Telecommunications Industry Association (TIA), is the CDMA standard developed by Qualcomm. CDMA currently provides 12-16 times the channel capacity over AMPS. CDMA has been implemented by a number of national wireless carriers, including, Verizon, and Sprint PCS. CDMA provides data services with rates of about 9.6 kbps. With CDMA, the frequency spectrum is shared by all calls. Each call is assigned a pseudo random code and the receiver in both the mobile phone and base station will only accept the call with the correct code.

- *Time division multiple access (TDMA).* TDMA is the generic name for an air interface technology that is used by a number of standard digital radio systems including IS-136 and GSM. The IS-136 standard is published by the TIA and is the current United States standard for both the cellular (850 MHz) and PCS (1.9 GHz) spectrums. TDMA has been implemented by a number of national wireless carriers including Cingular and AT&T Wireless. (In 2003 Cingular started transitioning many of their TDMA customers over to their new GSM system.) Each communications channel is divided into six time slots with two being used for each wireless connection. TDMA provides a three to one gain in network capacity over an analog cellular network and data rates of about 9.6 kbps. (IS-136 is also known as D-AMPS or Digital-AMPS.)

- *Iridium*. The Iridium satellite phone system is a TDMA system but it does not operate in the cellular frequency band.

- *Global System for Mobile communications* (*GSM).* GSM is the primary digital wireless phone standard throughout the world, except for primarily North America and Japan. The 3rd Generation Partnership Project (3GPP) of the European Telecommunication Standards Institute (ETSI), a European standards group, manages the GSM standard. GSM is a form of TDMA, but it has a different timing standard than the IS-136 version of TDMA. Security features, including customer billing, authentication information, and data encryption are recorded on a Subscriber Identity Module (SIM) card, which must be inserted into the phone before a call can be sent or received. The standard GSM data rate is 9.6 Kbps, but this capacity can be upgraded to 14.4 Kbps. T-Mobile (formerly VoiceStream), AT&T, and Cingular operate GSM networks in the U.S.

- *Integrated Dispatch Enhanced Network (iDEN).* iDEN is a TDMA based digital wireless phone technology that is used by Nextel for their nationwide wireless telephone service. iDEN is a proprietary specification that was developed by Motorola and integrates four wireless services into one digital network—dispatch radio, voice, data, and short message service (SMS). Nextel operates the only iDEN system in the U.S.

3.2.1.2 2.5 Generation (2.5G) Technologies

General Packet Radio Service (GPRS) is a packet-based digital wireless service and is considered an interim phase for GSM networks transitioning to 3G wireless systems. GPRS is deployed over GSM networks by overlaying a packet based air interface over the existing circuit-switched network. A version of GPRS has also been developed for IS-136 networks, but most U.S. based wireless carriers are using a GSM network as the foundation for their GPRS service. GPRS has maximum theoretical data rate of 171.2 Kbps with a typical user throughput of 56 – 115 Kbps. GPRS is considered an interim step from the transition of 2G wireless services to 3G. Cingular and T-Mobile (formerly VoiceStream) are among the U.S. wireless carriers that have deployed GPRS service to selected markets. The European Telecommunications Standards Institute (ETSI) maintains the GPRS standard.

3.2.1.3 3rd Generation (3G) Technologies

Universal Mobile Telecommunications System (UMTS) is the International Telecommunications Union's (ITU) IMT-2000 vision for a global family of 3G wireless communications systems and consists of five 3G wireless communications standards:

- IMT-2000 CDMA Direct Spread (DS), also known as the Universal Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) and includes WCDMA (or W-CDMA) which stands for Wideband Code Division Multiple Access. The 3rd Generation Partnership Project (3GPP) develops the Universal Mobile Telecommunications System (UMTS) and UTRA.

- IMT-2000 CDMA Multi-Carrier (MC), also known as cdma2000 (3X) was developed by 3GPP2. IMT-2000 cdma2000 includes 1X components (e.g., cdma2000 1X EV-DO).

- IMT-2000 CDMA Time Division Duplex (TDD), also known as UTRA TDD and Time Division - Synchronous Code Division Multiple Access (TD-SCDMA). TD-SCDMA was developed in China and is supported by the TD-SCDMA Forum.

- IMT-2000 TDMA Single Carrier, also known as UWC-136 Enhanced Data Rates for GSM Evolution (EDGE) which is supported by Universal Wireless Communications Consortium (UWCC).

- IMT-2000 Digital Enhanced Cordless Telecommunications (DECT) which is supported by the DECT Forum.

The IMT-2000 family of 3G systems includes three types of Core Network technologies:

- GSM based (using Mobile Application Part (MAP) protocols on top of SS7 protocols for signaling)

- ANSI-41 based (IS-634 protocols for signaling)

- Internet Protocol (IP) based

In the U.S., TDMA and GSM carriers will transition to EDGE while CDMA carriers plan to deploy either CDMA 2000 or WCDMA systems. CDMA2000 and WCDMA (UMTS) were developed separately and are two separate ITU approved 3G standards.

EDGE is a TDMA based 3G wireless radio interface standard that provides a migration path for GSM and IS-136 networks to 3G services. EDGE is the standard for IMT-2000 Single Carrier (also called Universal Wireless Communications-136 (UWC-136) and provides three to four times the data rates and throughput over GPRS (up to 384 Kbps theoretical with 115 Kbps considered the typical user data rate). Cingular, AT&T Wireless, and T-Mobile have announced plans to use EDGE for their 3G wireless services. The EDGE standard is supported by both the ITU and ETSI.

NOTE: EDGE is essentially a relatively low cost upgrade for a GSM carrier when compared to other 3G upgrades. This is why most U.S. TDMA carriers, including Cingular, started transitioning their customers to GSM networks in late 2002 and early 2003.

- CDMA 2000 is a trademark of the TIA and has been proposed as the IMT-2000 Multi Carrier standard. CDMA2000 1xRadio Transmit Technology (1xRTT), cdma2000 1xEvolution, Data Only (1xEV-DO) and future CDMA2000 3x were developed to be backward compatible with cdmaOne. Both 1x types have the same bandwidth and chip rate and can be used in any existing 2G cdmaOne frequency band and network. Backward compatibility was a requirement for successful deployment for the USA market. Deployment is straightforward because operators do not need new frequencies. Two interim versions of CDMA 2000 have been deployed or will be piloted in the United States:

  - 1xRTT CDMA will support up to 144 Kbps packet data in its first release and up to 614 Kbps in the second release. The second phase, 3x, completes the 3G evolution of the IS-95 CDMA standard. Verizon and Sprint PCS are deploying 1xRTT CDMA systems in select U.S. markets.

- 1xEV-DO (1x Evolution Data Only) is an enhancement to cdma2000 air interface technology optimized for packet data transfer. It is one of the most promising techniques for enabling third-generation (3G) wireless communications systems to deliver IP-based services such as e-mail, Web browsing, e-commerce and telematics. 1xEV-DO technology allows a standard 1.25 MHz cdma2000 wireless communication channel to provide a peak data rate of 2.4 Mb/sec on its forward link, effectively tripling the capacity of each CDMA2000 channel. Verizon has been testing 1xEV-DO networks in several locations in the U.S. 1xEV-DO offers an "always on" user experience, so that users are free to send and receive information from the Internet and their corporate intranets, anytime, anywhere.

- Wideband Code Division Multiple Access (WCDMA) is another approved 3G standard developed by DoCoMo, the dominate Japanese wireless carrier. WCDMA provides data rates up to 2 Mbps and will be piloted by AT&T in several locations in the United States. WCDMA (UMTS) was developed mainly for countries with GSM networks, because these countries have agreed to free new frequency ranges for UMTS networks. Because it is a new technology and in a new frequency band, new radio access networks have to be built. The advantage is that the new frequency band gives plenty of new capacity for operators. 3GPP is overseeing the standard development and has kept the core network as close to the GSM standard as possible.

3.2.1.4 Other Important Telephone Standards

ANSI 41 (with Revisions A, B, C, and D) is the industry standard for intersystem networking. This provides standards for communications between separate wireless carriers to support seamless roaming by wireless subscribers. Revision D provides the means to validate a wireless phone’s MIN and ESN before a roaming call is connected. This is the method that all wireless carriers in the U.S. use to authenticate/validate a phone prior to setting up a wireless phone call.

3.2.2 SMS Technology Overview

SMS is a standard protocol for GSM systems. TDMA and CDMA carriers are using several different, and in many cases, proprietary SMS protocols. Several U.S. wireless carriers are now providing messaging services that allow a user to send an SMS to another user on a competitor’s wireless network. SMS is used to transmit short messages between wireless phones and provides no security features. Although all digital wireless carriers encrypt data between the phone and the carrier base station, SMS messages are not normally encrypted as they transit the wireline network.

Multimedia Messaging Service (MMS) is an advanced form of SMS that provides the capability to transmit photos, graphics, video, and other forms of multimedia.

Wireless two-way messaging services are sold by a number of wireless vendors including cellular, wireless data, and two-way paging service providers. SMS services are rarely sold as a stand-alone wireless service and are usually bundled with wireless phone, data, or e-mail services.

3.2.3 Wireless Two-way Paging

Wireless pagers have almost become a technology of the past, having been replaced by wireless phone messaging services. Some vendors offer paging services with two-factor authentication and FIPS 140-2 compliant 128-bit 3DES encryption. Currently, no vendors offer two-way pagers and their associated services that provide an assured channel employing NSA Type-1 certified end-to-end encryption.

3.2.4 Cell Phone Security

No cellular radio transmission is completely secure, but digital and Personal Communications Service (PCS) phones are more secure than analog phones. Conversations on analog phones can be intercepted and decoded on inexpensive and readily available radio scanners. However, conversations on digital phones are encoded, which makes them more difficult to decode when intercepted.

- Smart cards were introduced in the wireless telephones by the GSM standard as Subscriber Identity Module (SIM) cards. SIM cards were designed as separate tokens located in cellular phones to hold and protect data and applications and to provide a barrier to subscription cloning. Over the years, SIM card functions have been enhanced and now provide secure user authentication and encryption services.

Several cellular phones are now available from General Dynamics and Qualcomm to secure sensitive and classified voice and data cellular communications and meet the NSA Type-1 certification requirements:

- The Motorola Sectéra Secure GSM (SGSM) cellular phone (available from General Dynamics) provides end-to-end high assurance security over commercial GSM cellular systems. The handset is designed to support hardware clip-in modules and is compliant with the Future Narrow Band Digital Terminal (FNBDT) standard. The Sectéra Security Module utilizes the NSA Type-1 certified security core developed for Motorola's Iridium® Security Module and Sectéra Wireline Terminal. The Sectéra Wireline Terminal provides secure voice and data when connected to a standard analog handset or PC and provides a transition from STU-III to FNBDT standards. This wireline terminal produces Type-1-4 encryption with PIN access.

- The Qualcomm QSec™-800 is the first cellular phone to provide end-to-end encrypted communications using existing, commercial cellular phone networks implementing CDMA data services. This phone provides high-grade voice security and normal cell phone operation in a single handset. The QSec™-800 offers secure interoperability with STE terminals that are based on the U.S. government's FNBDT-compliant technology and equipment.

- The QSec®-2700 is a new secure cellular phone from Qualcomm. The phone provides NSA Type-1 certified secure-voice communications and secure-data connectivity and operates over 800 MHz and 1900 MHz CDMA commercial wireless networks. In addition, the QSec 2700 provides a variety of 3G CDMA2000 1X technology wireless features with data speeds up to 153 Kbps.

3.2.5 Cell Phone Compliance Requirements

These requirements apply to single function cellular phones, PCS phones, SMS devices, and 2-way pagers and to multifunctional cellular devices (e.g., voice, SMS, MMS and 2-way pagers).

3.2.5.1 Classified Information

- *(WIR0350: CAT I) The IAO will ensure only NSA Type-1 certified cellular or satellite phones are used for classified voice or classified data wireless telephone transmissions. The classification level of information transmitted over the phone will not exceed the classification level approved for the phone.*

- *(WIR0360: CAT III) The IAO will ensure PEDs (PDA, cellular telephones, and wireless two-way email devices such as the BlackBerry) are not permitted in a permanent, temporary, or mobile SCIF unless approved by local site SCIF policies that are compliant with Director of Central Intelligence Directive (DCID) 6/9 and DCID 6/3.*

- *(WIR0370: CAT II) The IAO will ensure cellular devices are allowed or operated in areas where classified discussions or data processing takes place only when:*

- *The DAA, in consultation with the CTTA, has approved cellular devices can be brought into the facility and/or used in the facility.*

- *The device's voice recording capability is rendered inoperable.*

- *The cellular devices are separated from the classified data equipment at a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *Wireless devices are not connected via hot-sync to a workstation in a SCIF.*

3.2.5.2 Unclassified Information

Most cellular devices that store, process, or transmit data do not meet the security requirements of *DODD 8100.2* for storing, processing, and transmitting unclassified information. Therefore, cellular devices that store, process, or transmit data will not be used unless the following conditions are met:

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0540: CAT III) The IAO will ensure the cellular device data features are used to send and receive unclassified routine/administrative type information only.*

- *(WIR0550: CAT III) The IAO will ensure the cellular device data features provide some type of data encryption for the wireless link.*

- *(WIR0030: CAT III) The IAO will ensure cellular devices connecting directly or indirectly (hot-sync) to the network are added to site SSAAs.*

- *(WIR0360: CAT II) The IAO will ensure PEDs (PDA, cellular telephones, and wireless two-way email devices such as the BlackBerry) are not brought into a permanent, temporary, or mobile SCIF unless approved by local site SCIF policies that are compliant with DCID 6/9 and DCID 6/3.*

- *(WIR0356: CAT II) The IAO will ensure PDAs or cellular devices with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.*

- *(WIR0371: CAT III) The IAO will ensure PDAs or cellular devices with digital cameras (still and video) are allowed in a DOD facility only if specifically approved by site physical security policies.*

The IAO will ensure 3G cellular data systems are protected as follows:

- *(WIR0020: CAT III) The IAO will ensure when using a 3G cellular wireless data system on a laptop computer, the security compliance requirements in Section 2.6.5, Broadband Wireless System Compliance Requirements, are followed.*

- *(WIR0020: CAT III) The IAO will ensure when using a 3G cellular wireless data system on a PDA, the security compliance requirements in Section 3.3.4, PDA Compliance Requirements, are followed.*

The voice component of a cellular call is rarely encrypted unless a Sectéra or Q-Sec phone is used. Similarly, voice communications from commercial cordless phones and two-way radios are not secure. Therefore, the following applies to cellular voice calls, cordless phones, and two-way radios:

- *(WIR0340: CAT III) The IAO will ensure if non-secure (devices are not FIPS 140-2 certified or NSA Type-1 certified) cellular phones, cordless phones, and two-way radios are used for voice communications, users are trained not to discuss sensitive information over these devices.*

3.2.6 Blackberry Wireless Two-way E-mail

Security guidance for Blackberry wireless two-way e-mail systems is located in Appendix C, *Blackberry Security*.

3.3 PDA Technologies, Protocols, and Security

PDAs can be categorized based on the OS that is used. Currently, Palm OS, developed by Palm, and Windows Mobile (formerly Win CE), developed by Microsoft, have the largest market share. Symbian, a joint venture between Ericsson, Motorola, Nokia, and Psion, developed a third operating system called Symbian OS, originally called EPOC. In addition, JAVA and Linux based PDAs are now available. Most PDA operating systems released since 2003 provide security application programming interfaces (APIs) that application developers can use to enhance the security of their applications.

PDA manufacturers include several security-related applications with their PDAs, including password protection of data and VPN and SSL clients. In addition, add-on products with enhanced authentication capabilities, including signature, voice, and token-based authentication and data and file encryption are available from third party vendors.

Enhanced encryption and authentication can be provided from the device to the content server by implementing Wireless Application Protocol (WAP) PKI, also known as Wireless PKI (WPKI). Through the use of digital credentials, a secure framework can be implemented to protect transactions. WPKI can also be implemented on WAP enabled cellular phones and smartphones.

3.3.1 PDA Device Security Capabilities

3.3.1.1 Palm Devices

The current versions of Palm OS (Version 5 Garnet and Version 6 Cobalt) have many enhanced security features compared to previous versions. These security features include:

- Built in Palm OS security APIs.

- Secure user authentication including support for biometrics and the Challenge Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), and Password Authentication Protocol (PAP). Palm OS allows users to specify a set of rules (e.g., password, biometric token) that must be met in order to access the device.

- Data integrity and confidentiality encryption (128 bit). RC4 and SH-1 are included in PALM OS. Several third party vendors incorporate other cryptographic algorithms, including AES, via the Palm OS security APIs.

- Signed code support. When implemented, only applications that have a valid digital signature may access certain data and resources.

- SSL 3.0 and VPN (IPSec and PPTP) support.

- Device password protection. Can be set to automatically lock the device on power off, at a specific time, or after a specific period of inactivity.

- Password protection for select records stored on the PDA.

- Device level authentication to networks via the PDA Flash ID, Mobile Access Number (MAN), or Electronic Serial Number (ESN).

- Certificate management APIs and support for X.509v3 certificates.

Palm OS also supports infrared, IEEE 802.11, Bluetooth, and cellular add-on modems that are built in features of many PDA devices. Palm OS Colbalt also provides extensive Bluetooth and Smartphone support.

3.3.1.2 Windows Mobile

Microsoft renamed their operating system for mobile handheld devices to Windows Mobile. The core operating system of Windows Mobile is Win CE 4.2. Windows Mobile 2003 has been released in three versions:

- Pocket PC 2003 – Features include storing and retrieval of e-mail, contacts, appointments; play multimedia files and games; exchange text messages with MSN Messenger; and browse the Web. Data can also be synchronized with a desktop computer. Pocket PC 2003 provides improved WiFi support compared to Pocket PC 2002 including Zero Configuration WiFi that is similar to Wireless Zero Configuration (WZC) in Microsoft XP. (See *Section 2.2.5.*)

- Pocket PC Phone Edition – Combines all the standard functionality of Pocket PC 2003 with that of a feature-rich mobile phone. Provides wireless Internet access via a connection through a wireless service provider.

- Smartphone – Integrates PDA-type functionality into a voice-centric handset. Designed for one-handed handset operation with keypad access to both voice and/or data features. Optimized for voice and text communications, wireless access to Outlook information, and encrypted browsing to corporate and Internet information and services.

Windows Mobile 2003 improves security over previous versions of the WinCE platform. Microsoft has included a long alphanumeric password, but configuration settings will still permit a four-digit PIN. A user is allowed only three guesses of the password before erasing all of the data in the device's memory. Secure remote access functionality is included in Windows Mobile, including PPTP, SSL, and WTLS.

Windows Mobile includes power-on password protection and support for SSL and Private Communication Technology (PCT), the CryptoAPI 1.0 application programming interface and Windows 2000 challenge/response authentication.

Smartphone supports code signing of applications whereby any application that is downloaded is assigned to one of three trust levels:

- Privileged Trust means the application has a valid signature and a certificate that allows it access to all system resources. Very few applications should need this level of trust.

- Unprivileged Trust means the application has a valid signature, but a less trusted certificate, which means access to system resources, is restricted. Most applications will operate at this level.

- Untrusted means the application is either not signed or the certificate is not recognized. If the Smartphone enforces code signing, then such an application will not be allowed to load onto the device.

Since Windows Mobile is built on the modular WinCE operating system, each device manufacturer (HP, Casio, etc.) has the option of choosing which features to implement, therefore, not every Windows Mobile security feature may be available in a specific Windows Mobile PDA or Smartphone.

3.3.1.3 Symbian OS

Symbian OS includes a multi-tasking multithreaded core, a user interface framework, data services enablers, application engines, and integrated Personal Interface Module (PIM) functionality and wireless communications. Symbian is actively working with emerging standards, such as Java 2 Platform, Micro Edition (J2ME), Bluetooth, WAP, Multi-media Message Service (MMS), Synchronization Markup Language (SyncML), IPv6, and Wide band CDMA (WCDMA).

Symbian OS is the common core of APIs and technology that is shared by all Symbian OS phones. Symbian OS includes a multi-tasking kernel, middleware for communications, data management and graphics, the lower levels of the GUI framework, and application engines. Symbian OS security includes full-strength encryption and certificate management; secure communications protocols (including HTTPS, WTLS, and SSL); and certificate-based application installation.

Substantial security features were added in Symbian OS Version 6.0 (and included in subsequent versions. Version 8.1 is the latest release), primarily in two modules—the cryptography module and the certificate management module. Security features include standard cryptography algorithms, hash key generation, random number generation, and certificate management. The certificate management module certificate lifecycle services include storage and retrieval of certificates, assignment of trust status to a certificate on an application-by-application basis, certificate chain construction and validation, and verification of trust of a certificate.

Support is initially limited to X.509 certificates along with a PKI X.509 (PKIX) certificate usage profile. The architecture allows for other certificate formats and profiles to be added.

Symbian's licensees include Ericsson, Samsung, Matsushita (Panasonic), Nokia, Siemens, and Sony.

3.3.1.4 Wireless Java

The Java Technology for the Wireless Industry (JTWI) Roadmap 1 specification defines the version of the Java operating system for mobile devices. The latest edition of the Java toolkit (J2ME Wireless Toolkit 2.0), used by developers to build wireless Java applications and Java operating system packages for PDAs, contains a set of security APIs that provide the following features:

- Permissions and Code Signing – These APIs verify that an application is signed with a trusted digital signature. Access to resources and network connections are granted based on the digital signature verification.

- Server Authentication.

- SSL and TLS data encryption services.

NOTE: Security features available in a specific wireless Java PDA will depend on what security features the PDA vendor has implemented.

3.3.1.5 Linux

Many PDA developers believe that Linux is a better choice for mobile devices than other mobile/wireless operating systems because the operating system supports numerous installation methods that work in many heterogeneous environments and needs smaller resources.

A wide range of security features are available in Linux PDAs because vendors can include any available Linux operating system authentication, access control, and encryption security component or include various Linux security applications in their product.

3.3.2 On-Device File Encryption

The first line of defense for protecting data stored in mobile devices is the power-on password that comes built into the device. The second line of defense is to encrypt the data on the device. This provides security against data compromise attacks that can take place when a malicious individual has physical access to a lost/stolen PDA. Several vendors offer products that encrypt selected applications, content, and passwords on the device and support AES 128-bit encryption. FIPS 140-2 certified PDA file/data encryption products are available from several vendors.

3.3.3 Wireless Application Security

Many vendors offer software development kits (SDKs) for developing security features for handheld devices including PDAs, smartphones, cellular phones, etc. Security features included in applications are dependent on the PDA OS, on which programming and content development options used (Java and J2ME, C, C++, Visual BASIC, WAP, JavaPhone, Smartphone, etc.), as well as by various vendors' security libraries. Palm, Microsoft, Symbian, RSA, and Certicom offer toolkits to facilitate wireless application development and security.

3.3.4 PDA Compliance Requirements

3.3.4.1 Classified Information

- *(WIR0009: CAT I) The IAO will ensure all classified wireless systems are approved by the DAA prior to installation and use for processing classified DOD information.*

- *(WIR0380: CAT I) The IAO will ensure PDAs used to transmit, receive, store, or process Classified data use NSA, Type 1 certified end-to-end encryption for data being transmitted, received, stored, or processed.*

- *(WIR0360: CAT I) The IAO will ensure wireless PEDs (PDA, cellular telephones, and wireless two-way email devices such as the BlackBerry) are not brought into a permanent, temporary, or mobile SCIF unless approved by local site SCIF policies that are compliant with DCID 6/9 and DCID 6/3.*

- *(WIR0390: CAT II) The IAO will ensure PDAs are not permitted in a permanent, temporary, or mobile SCIF unless approved by Director Central Intelligence Directive (DCID) 6/9 or 6/3.*

- *(WIR0400: CAT I) The IAO will ensure PDAs are permitted in an area where classified data is discussed or processed only when:*

- *The DAA, in consultation with the CTTA, has approved PDAs can be brought into the facility and/or used in the facility.*

- *The PDAs are separated from the classified data equipment a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *The device's voice recording capability is rendered inoperable.*

- *(WIR0410: CAT II) The IAO will ensure PDAs are not connected to any workstation that stores, processes, or transmits classified data.*

- *(WIR0420: CAT II) The IAO will ensure synchronization software is not loaded on systems processing classified information. (Classified information will not be synched. PDAs will not be connected via hot-sync to a classified workstation.)*

- *(WIR0425: CAT II) The IAO will ensure classified data stored on PEDs is encrypted using NSA Type 1 certified encryption consistent with the classification level of the data stored on the device.*

- *(WIR0356: Category II) The IAO will ensure PDAs or cellular devices with digital cameras (still and video) are not allowed in any area where classified documents or information is stored, transmitted, or processed.*

3.3.4.2 Unclassified Information

- *(WIR0010: CAT I) The IAO will ensure all unclassified wireless systems are approved by the DAA prior to installation and use for processing unclassified DOD information.*

- *(WIR0012: CAT I) The IAO will ensure only DAA approved peripheral devices, operating systems, applications, and network/PC connection methods and wireless services are used.*

- *(WIR0050: CAT I) The IAO will ensure JTF-GNO approved anti-virus software is installed on all PDAs and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.*

- *(WIR0011: CAT III) The IAO will ensure no personally owned PED/PDAs are used to transmit, receive, store, or process DOD information.*

- *(WIR0371: CAT II) The IAO will ensure PDAs or cellular devices with digital cameras (still and video) are allowed in a DOD facility only if specifically approved by the site physical security policies.*

- *(WIR0450: CAT I) The IAO will ensure password protection, which meets the following requirements, is used to protect access to device data and applications.*

- *A password meeting DOD password policies is used, if this capability is available, and the password is changed at least every 90 days.*

- *The password protection feature will not permit its bypass without zeroing all data stored on the device.*

- *The password protection feature is enabled at all times.*

- *(WIR0460: CAT II) The IAO will ensure tools are used to encrypt data at rest on the wireless device. Encryption tools must be FIPS 140-2 certified.*

- *(WIR0465: CAT II) The IAO will ensure mobile code is not downloaded from non-DOD sources and is downloaded from only trusted DOD sources over assured channels.*

- *(WIR0470: CAT II) The IAO will ensure that PDAs that are used in areas where DOD information is processed:*

- *Have IR ports disabled when IR transmissions are not being used.*

- *Data exchange via the IR port should be limited to trusted DOD devices.*

- *The local CSA CTTA should be consulted to determine appropriate method for disabling the IR port on the PDA.*

Synchronization of wireless and handheld devices with applications or data located on a workstation or server (e.g., Microsoft Outlook) via a hot-sync cable or cradle can expose the DOD to significant security risks. Some synchronization systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the synchronization application on the workstation. Therefore, the following procedures will apply:

- *(WIR0480: CAT II) The IAO will ensure all PDA hot-sync operations meet the following conditions:*

- *Hot-sync management software uses some form of access control (e.g., user password must be entered before a hot-sync operation can be executed).*

- *The user disables wireless operations when a PDA is connected to the DOD wired network via a hot-sync or other interface cable.*

- *PDAs that transmit, receive, store, or process DOD information are not synced to home or personally owned PCs.*

- *(WIR0490: CAT II) The IAO will ensure PDAs used for wireless Internet remote access to DOD networks meet the following standards and criteria:*

- *Data encryption meeting the FIPS 140-2 (3DES or AES) standard is used on the device.*

- *PKI certificates are used for identification and authentication (I&A) of users.*

- *Only DAA approved PDAs, wireless service providers, and network access gateways are used.*

- *PDA wireless modems (e.g., IEEE 802.11, cellular, etc.) are removed or turned off when wireless data connections are not being used.*

- *JTF-GNO approved anti-virus software is installed on the device and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.*

- *A personal firewall is implemented on the device.*

PDA devices should only be purchased after verifying that file encryption software is available for that equipment. PDAs that will be used for wireless Internet remote access to DOD networks should only be purchased after it has been verified that FIPS 140-2 certified data encryption software, anti-virus software, and personal firewall software is available for that equipment. PDAs with Bluetooth radios should not be purchased unless the Bluetooth radio transmission can be secured with FIPS 140-2 certified data encryption software or the Bluetooth radio can be removed or disabled.

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Applicable Federal Policies and Guidelines

Current and Future Requirements for Federal Wireless Services in the United States, December 2001. (http://www.fwuf.gov/docs/rev_dec01.pdf)

Federal User's Wireless Telephone Security Risks *(*http://www.fwuf.gov)

FCC Rule 22.919, "Cellular Fraud"
(http://wireless.fcc.gov/services/cellular/operations/fraud.html)

NIST Special Publication 800-46 "Security For Telecommuting and Broadband Communications," Sept 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Device, November 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

OMB Circular A-130, Management of Federal Information Resources
(http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

Federal Communications CFR, Title 47, Part 15
(http://www.access.gpo.gov/nara/cfr/waisidx_00/47cfr90_00.html)

NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management
January 2000 Edition with 2001 Revisions
(http://www.army.mil/spectrum/library/regulations.htm)

Applicable DOD Policies and Guidelines

Enclave Security STIG

Network Infrastructure STIG

DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), 14 April 2004.

DOD Directive 8500.1, Information Assurance, 24 October 2002.

Director's Policy Letter 2003-7, Portable Electronic Devices, 1 July 2003.

DOD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

Office of the Secretary of Defense Memorandum, Department of Defense (DOD) Information Assurance Vulnerability Alert (IAVA).

OASD C3I Memorandum, Defense-wide Information Assurance Program Implementation Plan, 12 February 1999.

OASD C3I Memorandum, Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network, 22 August 1999.

DOD Directive 8100.1, Global Information Grid (GIG) Overarching Policy, 19 September 2002.

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, January 2000.

DISA CIO Guideline, Guidelines for S/MIME BlackBerry Orders, 16 December 2002.

DISA CIO Memorandum, Deployment of the Secure Multipart Internet Mail Extensions (S/MIME) Blackberry Device.

Draft CNSS Instruction 3034, Operational Security Doctrine for the SecNet-11 Wireless Local Area Network Interface Card.

The following industry and professional groups are involved in developing and/or sponsoring the development of wireless and wireless security standards:

Formal Standards Groups

American National Standards Institute (ANSI)
European Telecommunications Standards Institute (ETSI)
International Standards Organization (ISO)
Institute of Electrical and Electronics Engineers (IEEE)
International Telecommunications Union (ITU)
National Information Assurance Partnership (NIAP)
Telecommunications Industry Association (TIA)

Government Agencies

FCC Homeland Security Policy Council
Federal Communications Commission (FCC)
Federal Wireless Policy Committee (FWPC)
Federal Wireless Users Forum (FWUF)
National Institute of Standards and Technology (NIST)
National Telecommunication Information Administration (NTIA)

Industry Associations

Bluetooth Special Interest Group (SIG)
CDMA Development Group (CDG)
Cellular Telecommunication and Internet Association (CTIA)
Electronic Industry Association (EIA)
GSM Association
Infrared Data Association (IrDA)
Internet Engineering Task Force (IETF)
Personal Communications Industry Association (PCIA)
WAP Forum
Wireless LAN Alliance (WLANA)

WEP Vulnerability Web Links

Intercepting Mobile Communications: The Insecurity of 802.11 – DRAFT.
By Nikita Borisov, UC Berkeley; Ian Goldberg, Zero-Knowledge Systems; David Wagner, UC Berkeley.
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, Revision 2.
By Adam Stubblefield, Rice University; John Ioannidis, AT&T Labs; Aviel D. Rubin, AT&T Labs.
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Weaknesses in the Key Scheduling Algorithm of RC4.
By Scott Fluhrer, Cisco Systems; Itsik Mantin, The Weizmann Institute; Adi Shamir, The Weizmann Institute.
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

An Initial Security Analysis of the IEEE 802.1x Standard.
University of Maryland, Department of Computer Science
Mishra, Arunesh and Arbaugh, William A.
http://www.cs.umd.edu/~waa/1x.pdf

This page is intentionally left blank.

APPENDIX B. IAVM COMPLIANCE

IAVM Wireless Related Notices

No notices at this time.

JTF-GNO Wireless Related Notices

Vulnerability Note #	Title	Date
106678	IEEE 802.11 wireless network protocol DSSS CCA algorithm vulnerable to denial of service	5/13/2004
107186	Multiple vulnerabilities in SNMPv1 trap handling	02/12/2002
238678	The zlib compression library is vulnerable to a denial-of-service condition	10/01/2004
317350	ISC DHCP contains a stack buffer overflow vulnerability in handling log lines containing ASCII characters only	06/22/2004
398025	Remote Buffer Overflow in Sendmail	03/03/2003
516825	Integer overflow in Sun RPC XDR library routines	03/18/2003
654390	ISC DHCP contains C Includes that define vsnprintf() to vsprintf() creating potential buffer overflow conditions	06/22/2004
749342	Multiple vulnerabilities in H.323 implementations	01/13/2003
854306	Multiple vulnerabilities in SNMPv1 request handling	02/12/2002
879386	Multiple buffer overflow vulnerabilities in QNX	06/12/2002
886796	Cisco Aironet AP1100 fails to provide universal login error messages thereby disclosing validity of user account	07/28/2003
897604	Sendmail address parsing buffer overflow	03/29/2003

Table B-1 JTF-GNO Wireless Related Notices

This page is intentionally left blank.

APPENDIX C. BLACKBERRY SECURITY

C.1 Blackberry Wireless Two-way E-mail Overview

The Blackberry wireless e-mail service has become the most prevalent wireless e-mail service in DOD primarily because it was the first to be certified as compliant with FIPS 140-1. There are no specific standards used for wireless e-mail services. Wireless phone carriers and e-mail service providers use a number of protocols, some of them proprietary, for their e-mail service. Some form of account verification and data encryption is provided by most wireless e-mail services.

The Blackberry wireless e-mail service redirects a user's e-mail to a handheld wireless device. The e-mail redirector application can be installed on the user's computer or Blackberry Enterprise Server (BES) software can be installed on a network server. All incoming e-mail is redirected, via the Internet, to the wireless e-mail gateway. The e-mail gateway then transmits the e-mail to the wireless device. The wireless e-mail gateway also sends a copy of any e-mail sent from the handheld device, also via the Internet, back to the user's e-mail server so that a copy of the e-mail can be placed in the user's outbox.

All Research In Motion (RIM) BlackBerry email devices are FIPS 140-2 certified and use 3DES encryption. Some newer models also have AES encryption (software version 4.0 and later). All current RIM Blackberry models are S/MIME capable. S/MIME provides end-to-end e-mail encryption when used in conjunction with DOD PKI, even if the sender or recipient is not a BlackBerry user.

C.2 Wireless Two-way E-mail Compliance Requirements

C.2.1 Classified Information

A Classified Message Incident (CMI) or "data spill" occurs when a classified email is inadvertently sent on an unclassified network and received on a Blackberry device. The Blackberry data wiping function is not considered sufficient to clear the device of classified information.

- *(WIRPED010: CAT II) The IAO will ensure that if a Classified Message Incident (CMI) occurs on a Blackberry device, the device is handled as a classified device and destroyed appropriately.*

- *(WIR0500: CAT I) The IAO will ensure wireless two-way e-mail devices are not used to send, receive, store, or process classified messages.*

- *(WIR0360: CAT II) The IAO will ensure wireless PEDs (PDA, cellular telephones, and wireless two-way email devices such as the BlackBerry) are not permitted in a permanent, temporary, or mobile SCIF unless approved by local site SCIF policies that are compliant with DCID 6/9 and DCID 6/3.*

- *(WIR0520: CAT II) The IAO will ensure two-way e-mail devices are not permitted or used in areas where classified data processing takes place unless:*

- *The DAA, in consultation with the CTTA, has approved the two-way e-mail device for entry and use in the facility and/or used in the facility.*

- *The two-way e-mail device is separated from the classified data equipment a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *(WIR0420: CAT II) The IAO will ensure hot-sync software is not loaded on computers processing classified information.*

C.2.2 Unclassified Information

RIM recently released version 4.0 of the BlackBerry software suite (BlackBerry Enterprise Server (BES), BlackBerry Handheld Software, and BlackBerry Desktop Software). Version 4.0 includes a number of new security features. DOD BlackBerry users should upgrade to the version 4.0 when feasible (new handheld devices, with BlackBerry Handheld Software version 4.0 are required to take advantage of all new security features). Version 4.0 also adds a number of new system wide security policies that the system administrator can automatically push to every BlackBerry device in the domain. In addition, RIM has also released a new S/MIME Support package (SSP), version 4.0.

- *(WIR0012: CAT I) The IAO will ensure only DAA approved devices, operating systems, applications, and network/PC connection methods and wireless services are used.*

- *(WIR0030: CAT III) The IAO will ensure wireless devices, which connect directly or indirectly (hot-sync) to the network, are added to site the SSAA.*

- *(WIR0050: CAT I) The IAO will ensure JTF-GNO approved anti-virus software is installed on all wireless BlackBerry devices and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signature every 14 days or less.*

- *(WIR0560: CAT III) The IAO will ensure no personally owned BlackBerry devices are used to transmit, receive, store, or process DOD information.*

- *(WIR0590: CAT II) The IAO will ensure only the S/MIME BlackBerry enterprise server e-mail redirector is used. The Blackberry desktop redirector will not be used.*

- *(WIR0465: CAT II) The IAO will ensure that mobile code is not downloaded from non-DOD sources and is downloaded from only trusted DOD sources over assured channels.*

- *(WIR0620: CAT II) The IAO will ensure a BlackBerry device, which is reported lost or stolen, the Blackberry system administrator sends a kill command to the device and then deactivates the device at the BlackBerry server.*

- *(WIR0630: CAT II) The IAO will ensure password protection, where a password must be entered in order to access device data and applications, is enabled, configured and enforced as follows:*

  - *The device password is set to five or more lower case characters. (Combinations of lower case characters, upper case characters, numbers, or special characters may also be used. Passwords with numbers only must be at least 6 characters long.) The BES must be configured to enforce this policy.*

  - *The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The BES must be configured to enforce this policy.*

  - *The password is changed at least every 90 days.*

- *(WIR0592: CAT III) The IAO will ensure all Blackberry devices are set to lock (timeout) after 15 minutes or less of inactivity.*

- *(WIR0593: CAT I) The IAO will ensure when a Blackberry Mobile Data Service (MDS) is used to provide user access to internal DOD network servers, NTLM or DOD PKI authentication is enabled and user access is restricted to authorized servers only.*

NOTE: Ensure that the proxy server is configured to properly filter and handle the MDS protocol if this service is used for internal DOD network web browsing.

- *(WIR0640: CAT II) The IAO will ensure a Blackberry device, which has a Bluetooth radio, applies the following Bluetooth controls:*

  - *The uses of Bluetooth for data transmissions (e.g. syncing to the desktop, transfer of data files, etc.) on Blackberry devices are disabled unless FIPS 140-2 encryption is used. The BES must be configured to enforce this policy.*

NOTE: Bluetooth for voice transmissions (e.g. Bluetooth ear bud) is allowed, however, the BES must be configured to enforce this policy.

This page is intentionally left blank.

APPENDIX D. LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Automated Information Systems
AMPS	Advanced Mobile Phone Service
ANSI	American National Standards Institute
API	Application Program Interface
ARP	Address Resolution Protocol
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
BRAN	Broadband Radio Access Network
C2	Level C Security for Computer Products (provides Discretionary Access Control [DAC])
C&A	Certification and Accreditation
CA	Certificate Authority
CCI	Co-channel Interference
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CDG	CDMA Development Group
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CF	Compact Flash
CGI	Common Gateway Interface
CHAP	Challenge Authentication Protocol
CICS	Customer Information Control System
CJCS	Chairman, Joint Chiefs of Staff
CMI	Classified Message Incident
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CRT	Display Monitor (Cathode Ray Tube)
CSA	Command, Service, and Agency
CSA	Cognizant Security Authority
CTIA	Cellular Telecommunications & Internet Association
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DAC	Discretionary Access Control
dBi	Decibel (measure of antenna gain in decibels)
DCID	Director of Central Intelligence Directive
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Data Encryption Standard

DH	Diffie Hellman
DISA	Defense Information Systems Agency
DISAI	DISA Instruction
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DOS	Denial of Service
DSAWG	Defense Security Accreditation Working Group
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAS	Extended Assistance Support
ECC	Eliptic Curve Cryptogrophy
EDGE	Enhanced Data Rate for Global Evolution
EIA	Electronic Industry Association
EIR	Equipment Identity Register
E-mail	Electronic Mail
EMS	Extended Maintenance Support
ESAF	External Subsystem Attachment Facility
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FNBDT	Future Narrow Band Digital Terminal
FSO	Field Security Operations
FWPC	Federal Wireless Policy Committee
FWUF	Federal Wireless Users Forum
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HSCSD	High-Speed Circuit-Switched Data
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol - Secure
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
iDEN	Integrated Dispatch Enhanced Network

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
IR	Infrared
IrDA	Infrared Data Association
ISA	Industry Standard Architecture
ISM	Industrial, Scientific, and Medical
ISO	International Standards Organization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunications Union
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Media Access Control
MBPS	Megabits Per Second
MD5	Message Digest 5
MIC	Message Integrity Check
MIN	Mobile Identification Number
MS-CHAP	Microsoft CHAP
MMS	Multi-Media Message Service
NETSEC	Network Security
NIC	Network Interface Card
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSO	Network Security Officer
NSA	National Security Agency
OCB	Offset Codebook
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open Systems Interface
OUS&P	Outside United States and Possessions

PAN	Personal Area Network
PAP	Password Authentication Protocol
PCI	Peripheral Component Interconnect
PCIA	Personal Communications Industry Association
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Service
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PIM	Personal Interface Module
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure X.509
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point Tunnel Protocol
RADIUS	Remote Access Dial-in User Service
R & D	Research and Development
RF	Radio Frequency
RFID	Radio Frequency Identification
RSN	Robust Security Network
SA	System Administrator
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SGSM	Secure GSM
SHA	Secure Hash Algorithm
SID	System Identifier
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network
SM	Security Manager
SMF	System Management Facility
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRR	Security Readiness Review
SRRDB	SRR Database
SSAA	System Security Authorization Agreement
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSN	Subsystem Name
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide

TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneling TLS
UMTS	Universal Mobile Telecommunications System
UNII	Unlicensed National Information Infrastructure
US&P	United States & Possessions
USB	Universal Serial Bus
VCTS	Vulnerability Compliance Tracking System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WCDMA	Wide band CDMA
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WID	Wireless Information Device
Wi-Fi	Wireless Fidelity
WIM	WAP Identity Module
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WLANA	Wireless LAN Association
WMAN	Wireless Metropolitan Area network
WPA	Wireless Protected Access
WPA2	Wireless Protected Access 2
WPAN	Wireless Personal Area Network
WPKI	WAP or Wireless Public Key Infrastructure
WRAP	Wireless Robust Authentication Protocol
WTLS	Wireless Transport Layer Protocol
WWAN	Wireless Wide Area Network
WWW	World Wide Web
WZC	Wireless Zero Configuration

This page is intentionally left blank.