



Department of Defense INSTRUCTION

NUMBER 8420.01

November 3, 2009

ASD(NII)/DoD CIO

SUBJECT: Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)) and the guidance in DoD Instruction 5025.01 (Reference (b)), establishes policy, assigns responsibilities, and provides procedures for the use of commercial WLAN devices, systems, and technologies to achieve and increase joint interoperability, appropriately protect DoD information, and enhance overall security to sufficiently protect DoD information by embracing open standards for WLAN devices, systems, and technologies.

b. Incorporates and cancels Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Memorandum (Reference (c)).

c. Specifies the minimum set of security measures required on WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store unclassified and classified information.

d. Provides guidance on establishing a wireless network intrusion detection capability for monitoring local area networks (LANs).

2. APPLICABILITY

a. This Instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

(2) WLAN devices, systems, and technologies developed by commercial Industry in compliance with the current Institute of Electrical and Electronics Engineers (IEEE) standard in IEEE Standard 802.11-2007 (Reference (d)), or the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 8802-11 (Reference (e)) for the international operational environment, that are used to store, process, receive, or transmit unclassified and classified information. Reference (d) incorporates IEEE 802.11a-1999 (Amendment 1), IEEE 802.11b-1999 (Amendment 2), IEEE 802.11g-2003 (Amendment 4), and 802.11i-2004 (Amendment 6), which will hereafter be referred to as “IEEE 802.11.” WLAN-enabled information systems that have direct or indirect connection to operational DoD networks (i.e., SECRET Internet Protocol Router Network (SIPRNet), Non-Secure Internet Protocol Router Network (NIPRNet)) are not exempt from this Instruction, except as noted. A PED that is capable of IEEE 802.11 connectivity will hereafter be referred to as a WLAN-enabled PED.

b. This Instruction does not apply to:

(1) Other wireless or cellular technologies (e.g., 2.5/3/4G cellular systems, IEEE 802.15 wireless personal area networking (WPAN) standards (Bluetooth, ultra-wideband (UWB), ZigBee), proprietary microwave communications systems, IEEE 802.16-based Worldwide Interoperability for Microwave Access (WiMAX) systems, receive-only pagers, global positioning system receivers, hearing aids, and personal life support systems).

(2) The use of external WLAN systems that are not DoD owned or operated, or that are provided by commercial entities (e.g., hotspots), not-for-profit entities, DoD employees or contractors at personal residences, Federal partners, or research, development, test and evaluation (RDT&E) environments.

(3) The detection segment of a PED (e.g., the laser used in optical storage media; between a barcode and a scanner head; or radio frequency (RF) energy between RF identification tags, both active and passive, and the reader and/or interrogator), in accordance with DoDD 8100.02 (Reference (f)).

(4) The use of other wired or wireless access technologies or services on the WLAN-enabled PED that are not compliant with IEEE 802.11 (e.g., non-IEEE 802.11 memory cards, non-IEEE 802.11 Personal Computer Memory Card International Association (PCMCIA) cards, non-IEEE 802.11 ExpressCards, cellular network interface cards, non-IEEE 802.11 Universal Serial Bus (USB) adapters).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Unclassified WLAN systems shall be standards-based and IEEE 802.11 compliant, employ certified RF communications functions for interoperability, and employ certified and/or

validated information assurance (IA) and cryptographic functions, in accordance with sections 1 and 2 of Enclosure 3 of this Instruction.

b. Unclassified WLAN-enabled PEDs shall use antivirus software, personal firewalls, data-at-rest encryption, and implement strong identification and authentication (I&A) (e.g., two factor, at a minimum) to access the device and the network, in a manner compliant with paragraphs 2.a and 2.b and section 3 of Enclosure 3 of this Instruction.

c. Classified WLAN systems shall:

(1) Employ National Security Agency (NSA)-approved encryption end-to-end, and be protected with strong physical security, in accordance with paragraphs 4.a and 4.b of Enclosure 3 of this Instruction.

(2) Secure the storage, processing, receipt, and transmission of information accessed using NSA-approved encryption with a key whose encryption strength is commensurate with the classification level of the information.

(3) Implement IA measures that are consistent with Committee on National Security Systems (CNSS) Policy No. 17 (Reference (g)), in accordance with paragraph 4.c of Enclosure 3 of this Instruction.

d. Classified WLAN-enabled PEDs shall use NSA, Type 1 encryption to protect classified data-in-transit and data-at-rest on PEDs, in accordance with paragraphs 4.a and 4.d of Enclosure 3 of this Instruction.

e. Unclassified and classified DoD wired and wireless LANs shall have a wireless intrusion detection capability that can be used to monitor WLAN activity and identify WLAN-related policy violations, implemented in accordance with section 5 of Enclosure 3 of this Instruction.

f. Unclassified and classified WLAN-enabled PEDs used to access DoD e-mail systems shall support the signing and encrypting of e-mail, in accordance with DoDI 8520.2 (Reference (h)).

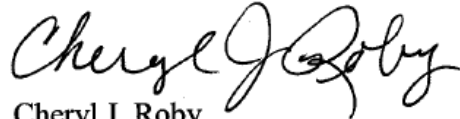
5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION REQUIREMENTS. The information requirements in this Instruction are exempt from licensing in accordance with sections C4.4.2 and C4.4.4 of DoD Manual 8910.1-M (Reference (i)).

8. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Directives Program Web Site at <http://www.dtic.mil/whs/directives>.

9. EFFECTIVE DATE. This Instruction is effective immediately.



Cheryl J. Roby
Acting Assistant Secretary of Defense for
(Networks and Information Integration)/
DoD Chief Information Officer

Enclosures

1. References
 2. Responsibilities
 3. Procedures
- Glossary

TABLE OF CONTENTS

REFERENCES6

RESPONSIBILITIES8

 ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION
 INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO).....8

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA)8

 DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA).....9

 DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
 (NSA/CSS).....9

 HEADS OF THE DoD COMPONENTS9

PROCEDURES.....11

 INDUSTRY STANDARDS COMPLIANCE FOR UNCLASSIFIED WLANS.....11

 UNCLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION.....12

 UNCLASSIFIED WLAN AUTHENTICATION APPROACHES.....15

 CLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION.....15

 WLAN INTRUSION DETECTION.....17

 WIRELESS SECURITY TECHNICAL IMPLEMENTATION (STIG) COMPLIANCE17

 WLAN SPECTRUM SUPPORTABILITY17

 INDUSTRY STANDARD WAVEFORM MODIFICATIONS.....18

 EXCEPTIONS TO THIS INSTRUCTION18

GLOSSARY20

 PART I: ABBREVIATIONS AND ACRONYMS20

 PART II: DEFINITIONS.....24

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (c) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Directive Type Memorandum (DTM) 06-007, "Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," June 2, 2006 (hereby canceled)
- (d) Institute of Electrical and Electronics Engineers Standard 802.11-2007, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," June 12, 2007¹
- (e) International Organization for Standardization/International Electrotechnical Commission 8802-11, Second edition, "Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," August 1, 2005²
- (f) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
- (g) Committee on National Security Systems Policy No. 17, "National Information Assurance (IA) Policy on Wireless Capabilities," August 2005
- (h) DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004
- (i) DoD Manual 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
- (j) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- (k) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
- (l) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990³
- (m) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
- (n) DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004

¹ Copies may be obtained at <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

² Copies may be purchased from the ISO Web site, <http://www.iso.org>

³ National Security Directive 42 may be obtained by SIPRNET subscribers via the NSA/CSS homepage, <http://www.nsa.smil.mil/>, under Information Assurance/IA Library/Presidential Issuances

- (o) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- (p) Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001
- (q) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage," July 3, 2007⁴
- (r) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (s) DoD Regulation 5200.08-R, "Physical Security Program," April 9, 2007
- (t) National Security Telecommunications and Information Systems Security Instruction No. 1000, "The National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000
- (u) Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 18, 2002⁵
- (v) Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
- (w) DoD Regulation 5200.1-R, "Information Security Program," January 14, 1997
- (x) DoD Wireless Security Technical Implementation Guide V5R2, "Wireless Security Technical Implementation Guide," November 15, 2007
- (y) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
- (z) DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004
- (aa) Military-Standard 461F, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," December 10, 2007
- (ab) Military-Standard 464A, "Electromagnetic Environmental Effects Requirements for Systems," December 19, 2002
- (ac) DoD Instruction 4630.09, "Wireless Communications Waveform Development and Management," November 3, 2008
- (ad) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (ae) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," June 2006

⁴ Approved for public release and distribution. Copies may be obtained by contacting ASD(NII)/DoD CIO.

⁵ Approved for limited distribution. Copies may be obtained by contacting the Office of the Intelligence Community Chief Information Officer.

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

- a. Monitor and provide oversight and policy development for all DoD WLAN activities.
- b. Establish a coordination process with the Intelligence Community (IC) Chief Information Officer (CIO) to ensure proper protection of IC information in implementing this Instruction.
- c. Assess potential WLAN system architectures. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics to ensure that the processes for acquisition of WLAN systems are clear and understandable, and address with the requirements of DoDD 5000.01 and DoDI 5000.02 (References (j) and (k), respectively).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall:

- a. Provide guidance for the development of incident response plans and standards for intrusion detection and intrusion prevention on DoD wired and wireless LANs.
- b. Develop and provide, in conjunction with Joint Staff Directorate for Command, Control, Communications, and Computer System, architectures, system requirements, and specifications to support WLAN solution interoperability and net-readiness testing.
- c. Develop and provide architectures, specifications, systems engineering, and integration guidelines for command and control capable WLAN systems in coordination with National Security Agency/Central Security Service (NSA/CSS), per National Security Directive 42 (Reference (l)), to support WLAN solution interoperability and net-readiness testing.
- d. Ensure that the Joint Interoperability Test Command (JITC) performs interoperability testing and provides interoperability certification of WLAN devices deployed within the Department of Defense, in accordance with DoDD 4630.05 (Reference (m)).

(1) Once an interoperability test is conducted, the results may be used to issue an interoperability certification, if the test criteria and configuration satisfy established requirements.

(2) JITC may also issue a DoD Standards Conformance Certification for WLAN-enabled PEDs that implement standards that may impact interoperability.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)), shall provide intelligence support and guidance on the use of WLAN technologies in a DIA-accredited Sensitive Compartmented Information Facility (SCIF).

4. DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE (NSA/CSS). The Director, NSA/CSS, under the authority, direction, and control of the USD(I), and pursuant to Reference (I) shall:

a. Develop medium and high assurance protection profiles for WLAN client systems, WLAN access systems, personal firewalls, antivirus protection packages, and wireless intrusion detection systems (WIDS).

b. Provide risk and vulnerability assessments for WLAN technologies that are responsive to DoD requirements.

c. Develop and disseminate threat information regarding the capabilities and intentions of adversaries to exploit WLAN technologies used by the DoD Components.

d. Serve as the DoD focal point for WLAN IA technology research and development, to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. As necessary, coordinate these activities with the Director, Defense Research and Engineering.

e. Function as the approval authority for Type 1 certification of commercial WLAN products.

5. HEADS OF THE DoD COMPONENTS. The Heads of DoD Components shall:

a. Ensure that all procurements of commercial WLAN products and subsequent operations comply with this Instruction.

b. Promote joint interoperability through the adoption of commercial, standards-based, IA-certified WLAN products in accordance with the requirements of this Instruction.

c. Control WLAN access to information systems to ensure that WLAN-based threats (including authorized and unauthorized WLAN devices, technologies, or systems) do not introduce vulnerabilities that undermine the assurance of the other interconnected systems.

d. Prepare and execute incident response plans for WLAN intrusion detection events.

e. Comply with all procedures identified in Enclosure 3.

f. Ensure all authorized users, privileged users, and IA managers of WLAN devices, systems, and technologies receive IA awareness training and are trained and certified to perform respective IA duties, in accordance with DoDD 8570.01 (Reference (n)).

ENCLOSURE 3

PROCEDURES

1. INDUSTRY STANDARDS COMPLIANCE FOR UNCLASSIFIED WLANS

a. Standards-Based WLAN Technologies. DoD Components shall ensure that only standards-based WLAN technologies are deployed for unclassified WLANS by adhering to:

(1) IEEE Standards. Only WLAN devices, systems, and technologies that are compliant with IEEE 802.11 shall be acquired.

(2) Internet Engineering Task Force (IETF) Standards. Only standards-based WLAN identification and authentication between WLAN devices and WLAN infrastructure that is in compliance with the IETF Extensible Authentication Protocol (EAP) request for comment (RFC) 4017 standard shall be provided. (Copies may be obtained at <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.) The IETF EAP-Transport Layer Security (EAP-TLS) RFC 2716 standard shall be used as the only approved EAP method. (Copies may be obtained at <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.)

b. WLAN System Interoperability. DoD Components shall ensure systems interoperability for unclassified WLANS by adhering to:

(1) Wireless Fidelity (Wi-Fi) Alliance Certification. All acquisitions of WLAN-enabled devices shall be Wi-Fi and Wi-Fi Protected Access 2 (WPA2) Enterprise certified by the Wi-Fi Alliance. WLAN-enabled devices (e.g., Network Interface Cards (NICs) and access points (APs), WLAN controllers, WLAN switches) that store, process, or transmit unclassified information shall be:

(a) Wi-Fi Alliance certified as 802.11a, 802.11b, 802.11g, 802.11n, or other 802.11 Physical (PHY)-Layer standards for device data communications interoperability. The Wi-Fi Alliance certifies that WLAN-enabled devices are able to negotiate PHY- and Media Access Control (MAC)-Layer specification data communications and can establish International Standards Organization (ISO) open systems interconnect (OSI) Layer 1 and Layer 2 connections.

(b) WPA2 Enterprise certified for device security communications interoperability. WPA2 certifies that WLAN-enabled devices that implement Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol (known collectively as AES-CCMP) are able to negotiate MAC-Layer specification security communications and can establish an ISO OSI Layer 2 security connection.

(2) JITC Approval. Per Reference (1), DoD Components shall ensure that systems meet overall end-to-end interoperability requirements as approved by the JITC. Obtaining Wi-Fi and

WPA2 interoperability certifications does not eliminate the requirement for obtaining JITC certification, in accordance with References (m) and (l).

2. UNCLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION. DoD Components shall ensure that unclassified WLAN products are certified and validated for secure end-to-end communications. Per DoDI 8510.01 (Reference (o)), DoD Components shall ensure that the system meets overall end-to-end security requirements as approved by the designated accrediting authority (DAA).

a. National Institute of Standards and Technology Certifications. Per Reference (f), encryption of unclassified data-in-transit via WLAN-enabled PEDs, systems, and technologies shall be implemented in a manner that protects the data end-to-end. All system components within a WLAN that wirelessly transmit unclassified DoD information shall have cryptographic functionality that is validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP), as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140 (Reference (p)). There are multiple FIPS 140 Publications (e.g., FIPS 140-1, FIPS 140-2, FIPS 140-3), which hereafter will be referred to collectively as “FIPS 140” to reference the currently approved publication. Per Reference (f), encryption of data-at-rest that is validated under the NIST CMVP as meeting FIPS 140 shall be implemented on WLAN-enabled PEDs.

(1) WLAN-Enabled PEDs. Unclassified WLAN-enabled PEDs shall have FIPS 140 validated encryption to protect data-in-transit on the WLAN client portion of the end-to-end WLAN communications link. WLAN-enabled PEDs may implement encryption either in software (via the WLAN supplicant) or in hardware (via the WLAN NIC).

(a) Software-Based Encryption. WLAN client supplicants supporting this configuration shall disable (or otherwise preempt) the encryption capabilities of the WLAN client’s NIC so that the encryption can be performed solely by the supplicant software. WLAN client supplicants shall implement the AES-CCMP for encryption as defined in Reference (d). The AES-CCMP encryption shall be validated under the NIST CMVP as meeting FIPS 140.

(b) Hardware-Based Encryption. WLAN client NICs supporting this configuration shall implement AES-CCMP as defined in Reference (d) within NIC hardware. The AES-CCMP encryption shall be validated under the NIST CMVP as meeting FIPS 140.

(2) AP/WLAN Controller. Unclassified WLAN infrastructure devices shall have FIPS 140 validated encryption to protect data-in-transit on the WLAN infrastructure portion of the end-to-end WLAN communications link. WLAN infrastructure systems may be composed of either stand-alone (also referred to as an autonomous) APs, or thin APs that are centrally controlled by a WLAN controller (also referred to as a WLAN switch). All WLAN infrastructure devices shall implement AES-CCMP as defined in Reference (d). The AES-CCMP encryption shall be validated under the NIST CMVP as meeting FIPS 140.

(3) Data-at-Rest. Data-at-rest encryption shall be implemented in a manner that protects unclassified information stored on WLAN-enabled PEDs by requiring that the PED must be powered on and credentials successfully authenticated in order for the data to be deciphered. Credentials for authentication shall be either public key infrastructure (PKI) certificates on the Common Access Card (CAC) or username/password for devices that cannot interface with the CAC. Data-at-rest encryption shall include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g., hard disks, on-board memory cards, memory expansion cards). In recognition of the increased risk of unauthorized access to unclassified information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption shall be provided for data-at-rest on all WLAN-enabled PEDs that is validated as meeting FIPS 140 Overall Level 1 or Level 2 requirements. All unclassified DoD data-at-rest on WLAN-enabled PEDs that has not been approved for public release shall be encrypted, in accordance with ASD NII/DoD CIO Memorandum (Reference (q)).

(4) WLAN Authentication. Unclassified WLAN systems shall have NIST CMVP FIPS 140 validated authentication schemes.

(a) WLAN Client Supplicant Authentication. Authentication shall be implemented by WLAN client supplicants that comply with IETF EAP standards for WLANs RFC 4017. The approved algorithms (e.g., Hash Message Authentication Code (HMAC), and Secure Hash Standard (SHS)) implemented during the EAP authentication process shall be validated under the NIST CMVP as meeting FIPS 140.

(b) Authentication Server. Authentication servers are responsible for authenticating user and/or device credentials during EAP authentication; some also transmit the keying information that enables the AES-CCMP 4-way handshake as defined in Reference (d). Reference (d) includes Remote Authentication Dial In User Service (RADIUS) (IETF RFC RFC 3579) as an authentication server, which is part of a WLAN system. Alternative authentication servers are available via proxy-type authentication in WLAN controllers that allow the WLAN infrastructure to authenticate against X.500 directories, lightweight directory access protocol (LDAP) services, domain controllers, local user databases, and other authentication sources. Authentication servers interconnect with WLAN infrastructure over the distribution (or backhaul) portion and not the access portion of the network. Therefore, the distribution portion does not represent the same level of risk to exposure of DoD information. Authentication servers transmit keying information once a user and/or device has been authenticated, which allows the WLAN client supplicant and AP to begin negotiating security keys for AES-CCMP data-in-transit encryption (Reference (d) calls the keying information the “authentication, authorization, and accounting (AAA) key”). The authentication server must transmit the keying information to the AP via a separate process. The secure transmission of keying information to APs is known as key wrapping. Some authentication servers are embedded within the WLAN infrastructure, and therefore can process keying information internally within the WLAN infrastructure. Also, some WLAN infrastructure has the ability to internally generate the keying information, thereby not requiring the transmission of keying information from authentication servers.

1. EAP-Authentication. DoD Components that implement authentication servers that generate keying information and implement EAP-authentication of credentials provided by

WLAN client supplicants shall implement approved algorithms (e.g., HMAC, SHS, random number generator (RNG), AES, and Rivest-Shamir-Adleman (RSA)) validated under the NIST CMVP as meeting FIPS 140.

2. Encrypted Key Wrapping. DoD Components that implement authentication servers that generate keying information and implement key wrapping prior to transmission to APs may validate the key wrapping under the NIST CMVP as meeting FIPS 140. The key wrapping shall be implemented with approved algorithms (e.g., AES) validated under the NIST CMVP as meeting FIPS 140.

(5) Validated Physical Security. APs used in unclassified WLANs should not be installed in unprotected environments due to an increased risk of tampering and/or theft. If installed in unprotected environments, APs that store plaintext cryptographic keying information shall be protected with added physical security to mitigate risks. DoD Components may choose products that meet FIPS 140-2 Overall Level 2, or higher, validation (to ensure that the AP provides validated tamper evidence, at a minimum). Alternatively, DoD Components may physically secure APs by placing them inside of securely mounted, pick-resistant, lockable enclosures.

b. National Information Assurance Partnership Validation. Any IA-enabled unclassified WLAN product shall be National Information Assurance Partnership (NIAP) Common Criteria (CC) validated. When available, WLAN-enabled solutions shall be validated under the NIAP CC as meeting applicable U.S. Government (USG) WLAN protection profiles (e.g., WLAN client or WLAN access system) for medium robustness environments, in accordance with DoDD 8500.2 (Reference (r)).

(1) WLAN Access Systems/Client Systems. WLAN-enabled PEDs and infrastructure (e.g., WLAN APs, WLAN controllers, WLAN NICs, and WLAN supplicants) shall be NIAP CC validated. WLAN devices and infrastructure shall be validated under the NIAP CC as meeting applicable USG WLAN access systems or client systems protection profiles for medium robustness environments, when products are available.

(2) Antivirus. WLAN-enabled PEDs shall use antivirus software when data services are to be used on those devices, per Reference (r). Antivirus software shall be NIAP CC validated as meeting the USG antivirus protection profile for medium robustness environments, when products are available.

(3) Personal Firewall. WLAN-enabled PEDs shall use personal firewalls, per Reference (r). Personal firewalls shall be NIAP CC validated as meeting USG personal firewall protection profile for medium robustness environments, when products are available.

(4) WIDS. DoD Components shall use WIDS to actively screen for unauthorized WLAN activity, per Reference (f). WIDS shall be validated under the NIAP CC as meeting applicable USG protection profiles for medium robustness environments, when products are available.

3. UNCLASSIFIED WLAN AUTHENTICATION APPROACHES. Per Reference (f), strong authentication shall be implemented at network and device levels as a method of protecting access to unclassified WLANs. DoD Components shall ensure that standards-based EAP authentication is used to authenticate unclassified WLAN users and/or devices.

a. Strong Identification and Authentication. Per Reference (f), unclassified WLAN devices, systems, and technologies shall use strong I&A (e.g., two factor, at minimum) at the device and network levels in accordance with published DoD policies and procedures. When “something you have” is used as one of the authentication factors, it shall be something other than the WLAN-enabled PED. Examples of the “something you have” authentication factor include, but are not limited to: key fobs, smartcards, USB tokens, and hardware tokens. Strong authentication at the device and network levels may be achieved by assessing the combined processes of WLAN authentication (e.g., 802.1X and EAP) and domain authentication (e.g., domain and/or directory login).

b. WLAN Authentication. DoD Components shall implement unclassified WLAN systems with standards-based authentication mechanisms. WLAN authentication is to be achieved by ensuring interoperability and validated secure implementations. WLAN authentication shall implement the AES-CCMP 4-way handshake key exchange as defined in Reference (d). WLAN devices and infrastructure shall be WPA2 Enterprise certified to ensure that authentication can be negotiated in a mixed vendor WLAN system implementation. WLAN infrastructure shall implement 802.1X access control to prevent WLAN access to unauthorized WLAN devices and enforce authentication of authorized WLAN devices, prior to providing access. EAP authentication shall facilitate the verification of credentials provided by authorized WLAN devices and/or users. Cryptographic modules implemented to facilitate authentication shall be FIPS 140 validated in accordance with paragraph 2 of this enclosure.

4. CLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION. DoD Components shall ensure that classified WLAN products are certified and validated for secure end-to-end communications. Per Reference (o), DoD Components shall ensure that the system meets overall end-to-end security requirements as approved by the DAA.

a. Certification of Classified WLAN Products. WLAN devices, systems, and technologies used to transmit, store, or process classified information shall:

(1) Be reviewed and certified by NSA prior to acquisition and use. In order for a product to be NSA-approved, the product must have its implementation, key and key management, concept of operations (CONOPS), and interoperability requirements independently certified by NSA.

(2) Use NSA-approved Type 1 products, appropriately keyed, for encrypting and decrypting classified and sensitive national security information. The NSA Commercial Communication Security (COMSEC) Evaluation Program (CCEP) is the approval authority for commercial products certified as Type 1.

b. Physical Security of Classified WLANs

(1) WLAN APs used to transmit or process classified information shall be physically secured, and methods shall exist to facilitate the detection of tampering. WLAN APs are part of communication systems and shall have controlled physical security, in accordance with DoD 5200.08-R (Reference (s)).

(2) Either physical or electronic inventories may be conducted by polling the serial number or MAC address. APs not stored in a COMSEC-approved security container shall be physically inventoried.

(3) WLAN APs shall be set to the lowest possible transmit power setting that meets the required signal strength of the area serviced by the AP.

c. Information Assurance for Classified WLANs. Implementation of classified WLAN devices, systems, and technologies shall:

(1) Be rekeyed every 90 days, at a minimum.

(2) Use a session timeout capability, not to exceed 30 minutes.

(3) Employ identification and authentication (I&A) measures for the WLAN-enabled PED and WLAN, in accordance with National Security Telecommunications and Information Systems Security Instruction No. 1000 (Reference (t)).

(4) Include integrity and non-repudiation controls.

(5) Support adjustments to operations and/or configurations based on guidance issued by the SIPRNET Connection Approval Office (CAO). Written operating procedure or policy shall describe procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material.

(6) Ensure that a SIPRNET connection approval package is on file with the CAO and the package is updated, as needed, to include the classified WLAN system.

(7) Not use WLAN devices in a permanent, temporary, or mobile SCIF unless approved in accordance with Director Central Intelligence Directive 6/9 (Reference (u)) or Intelligence Community Directive Number 503 (Reference (v)) requirements.

(8) Ensure that the Certified TEMPEST Technical Authority (CTTA) is notified before installation and operation of WLANs intended for use in processing or transmitting classified information.

(9) Ensure that all WLAN systems are certified and accredited, in accordance with References (o) and (t).

(10) Configure APs to perform client device access control using MAC filtering.

d. Protection of Classified Data-At-Rest on WLAN-Enabled PEDs. Classified data-at-rest on PEDs shall be protected by:

(1) Implementing encryption of classified data-at-rest with NSA Type 1 certified encryption at a level consistent with the classification of the data stored on the device;

(2) Removing storage media that contains classified information from the PED and storing it within the appropriate General Services Administration (GSA)-approved security container, in accordance with DoD Regulation 5200.1-R (Reference (w)); or

(3) Placing the entire PED within the appropriate GSA-approved security container, in accordance with Reference (w).

5. WLAN INTRUSION DETECTION. DoD Components shall ensure that a WIDS is implemented that allows for monitoring of WLAN activity and the detection of WLAN-related policy violations on all unclassified and classified DoD wired and wireless LANs.

a. WIDS Monitoring Requirements. The WIDS shall be capable of monitoring IEEE 802.11 transmissions within all DoD LAN environments and detect nearby unauthorized WLAN devices. WIDS shall not be required to monitor non-IEEE 802.11 transmissions.

b. WIDS Implementation Criteria. The WIDS shall continuously scan for and detect authorized and unauthorized WLAN activities 24 hours a day, 7 days a week. Scanning shall include a location-sensing capability that enables designated personnel to locate, identify, and take appropriate actions to mitigate IEEE 802.11 threats.

6. WIRELESS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) COMPLIANCE. In addition to adhering to the procedures specified in this enclosure, incorporate the security best practices specified in the Wireless STIG (Reference (x)), as it pertains to the implementation of WLANs.

7. WLAN SPECTRUM SUPPORTABILITY. Ensure spectrum supportability prior to acquiring spectrum-dependent WLAN systems in accordance with DoDD 4650.01 (Reference (y)), and ensure compliance with the DoD Electromagnetic Environmental Effects Program in accordance with DoDD 3222.3 (Reference (z)). Ensure adherence with Military Standards (MIL-STD) that are applicable to the installation and operation of WLANs, in accordance with MIL-STD 461F and MIL-STD 464A (References (aa) and (ab)). The Department of Defense requires that non-licensed devices operating in the United States and its possessions (USP) shall be registered with the local spectrum management office. Outside USP, each theater commander and host nation shall determine if frequency support is available and authorized. Users must submit a

DD Form 1494, "Application for Equipment Frequency Allocation," through the supporting spectrum management office for equipment that intentionally radiates and will be deployed outside the USP. After obtaining favorable host nation guidance, users may request frequency assignment, as needed.

8. INDUSTRY STANDARD WAVEFORM MODIFICATIONS. To ensure system and network interoperability, unclassified and classified WLAN communications waveforms that are not in full compliance with open commercial standards shall be subject to review and assessment by ASD(NII)/DoD CIO. Waveform development and modifications (e.g., spectrum, power output level, symbol, throughput modulation, or coding modifications) must be submitted for review and assessment in accordance with the procedures specified in DoDI 4630.09 (Reference (ac)).

9. EXCEPTIONS TO THIS INSTRUCTION

a. Unclassified WLAN Security Exceptions. DAAs are authorized to grant exceptions to this Instruction for unclassified WLAN devices, systems, or technologies.

(1) Non-Compliant WLAN Devices, Systems, or Technology Exceptions. Exceptions may be made by the DAA for the use of non-compliant WLAN devices, systems, or technologies provided the justification for the exception is documented as part of the system's DoD Information Assurance Certification and Accreditation Process (DIACAP) package, in accordance with Reference (o). The documentation shall denote acceptance of a non-standard security solution and the potential impact that a loss of interoperability imposes on the system, DoD users, and the Global Information Grid (GIG). DAAs shall review the DIACAP package to make an informed decision about the impact to interoperability before granting an exception.

(a) Exceptions for the Use of Type-1 Devices on Unclassified WLANs. Use of NSA-certified Type 1 products is also acceptable for unclassified data, when operating in the secure mode. Type 1 WLAN products are proprietary in nature and are not interoperable with IEEE 802.11 solutions, and therefore represent a loss of interoperability.

(b) Exceptions for Minimal Impact WLAN Systems. Exceptions can be granted by the DAA for minimal impact WLANs systems. Minimal impact WLANs systems are systems that: do not provide connectivity to WLAN-enabled PEDs (e.g., backhaul systems); have no available FIPS 140 validated, 802.1X, EAP-TLS supplicant; support a very small number of users for a specific mission (i.e., 10 or less users); are standalone networks; or are highly specialized WLAN systems that are isolated from the GIG (e.g., handheld personal digital assistants (PDAs) used as radio-frequency identification (RFID) readers, a network of WLAN-enabled Voice over Internet Protocol (VoIP) phones). These systems shall be segmented from the GIG via a wireless demilitarized zone (DMZ) that provides network intrusion detection capabilities and limits ports and protocols to the minimum set necessary to achieve mission objectives. A STIG-compliant firewall shall be located at the system's point of entry onto the GIG.

(2) Unclassified WLAN Backhaul Exceptions. WLAN technologies that are deployed solely to establish backhaul or site-to-site connectivity (i.e., bridge links that do not directly interconnect with user devices) via point-to-point or point-to-multipoint links are exempt from the standards set forth in this Instruction. DoD Components shall protect backhaul data-in-transit with FIPS 140 validated encryption modules in accordance with Reference (f).

(3) Unclassified WIDS Exceptions. Exceptions to WIDS implementation criteria stated in this Instruction may be made by the DAA for DoD wired and WLANs operating environments. This exception allows the DAA to implement periodic scanning conducted by designated personnel using handheld scanners during walkthrough assessments. Periodic scanning may be conducted as the alternative to the continuous scanning described in paragraph 5.b of this enclosure only in special circumstances where it has been determined on a case-by-case basis that continuous scanning is either infeasible or unwarranted.

b. Classified Exceptions. Exceptions are not authorized for classified WLAN devices, systems, or technologies, or WIDS.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

2.5G	2.5 generation cellular wireless technology
3G	3rd generation cellular wireless technology
4G	4th generation cellular wireless technology
802.1X	IEEE Standard for Port-based Network Access Control
802.11-2007	IEEE WLAN Standard, Maintenance & Revision
802.11a	IEEE WLAN Standard for Higher Speed PHY Extension in the 5GHz Band, also known as IEEE Std. 802.11-2007 (formerly IEEE 802.11a-1999 (Amendment 1)).
802.11b	IEEE WLAN Standard for Higher Speed PHY Extension in the 2.4 GHz Band, also known as IEEE Std. 802.11-2007 (formerly IEEE 802.11b-1999 (Amendment 2)).
802.11g	IEEE WLAN Standard for Further Higher Data Rate Extension in the 2.4 GHz Band, also known as IEEE Std. 802.11-2007 (formerly IEEE 802.11g-2003 (Amendment 4)).
802.11i	IEEE WLAN Standard for MAC Security Enhancements, also known as IEEE Std. 802.11-2007 (formerly IEEE 802.11i-2004 (Amendment 6)).
802.11n	IEEE WLAN Standard for High Throughput
802.15.1	IEEE WPAN Standard (also known as Bluetooth)
802.16	IEEE WiMAX Standard for ETSI HIPERMAN and Mobile WiMAX
AAA key	authentication, authorization, and accounting key
AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) Protocol
AP	access point
ASD NII/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CAC	Common Access Card
CBC	cipher block chaining
CC	common criteria

CCEP	Commercial COMSEC Evaluation Program
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
COMSEC	communication security
CONOPS	concept of operations
CTTA	Certified TEMPEST Technical Authority
DAA	designated accrediting authority
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DoDD	DoD Directive
DoDI	DoD Instruction
DTM	Directive-type memorandum
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
FIPS	Federal Information Processing Standards
GHz	gigahertz
GIG	Global Information Grid
GSA	General Services Administration
HMAC	Hash Message Authentication Code
I&A	identification and authentication
IA	information assurance
IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Standards Organization

ISO/IEC	International Standards Organization/International Electrotechnical Commission
IT	information technology
JITC	Joint Interoperability Test Command
LAN	local area network
LDAP	lightweight directory access protocol
MAC	Message Authentication Code
MAC-Layer	medium access control layer
MIL-STD	Military Standard
NIACAP	The National Information Assurance Certification and Accreditation Process
NIAP	National Information Assurance Partnership
NIC	network interface card
NIPRNET	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security Systems
OSI	Open Systems Interconnection
PCMCIA	Personal Computer Memory Card International Association
PDA	personal digital assistant
PED	portable electronic device
PHY-Layer	physical layer
PK	public key
PKI	public key infrastructure
RADIUS	Remote Authentication Dial In User Service
RDT&E	research, development, test and evaluation
RF	radio frequency
RFC	request for comments

RFID	radio-frequency identification
RNG	random number generator
RSA	Rivest-Shamir-Adleman
SCIF	Sensitive Compartmented Information Facility
SHS	Secure Hash Standard
SIPRNET	SECRET Internet Protocol Router Network
STIG	Security Technical Implementation Guide
Std.	standard
USB	Universal Serial Bus
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. Government
USP	United States and its possessions
UWB	ultra-wideband
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WIDS	wireless intrusion detection system
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless local area network
WPA2	Wi-Fi Protected Access 2
WPAN	wireless personal area network

PART II. DEFINITIONS

Unless otherwise noted, the following terms and their definitions are for the purposes of this Instruction.

AES-CCM. An encryption algorithm that utilizes the 128-bit block ciphers to provide authentication and privacy.

IEEE 802.1X. An IEEE standard that performs network access control by utilizing EAP to provide authentication to LAN devices.

IEEE 802.11. An IEEE body of standards that operate in the 2.4 GHz and 5 GHz spectrum bands in order to provide communication in WLAN environments. The family of standards is comprised of the IEEE Std. 802.11-2007 (which incorporates 802.11a, 802.11b, 802.11d,

802.11g, 802.11h, 802.11i, 802.11j, 802.11e) and a number of amendments (e.g., 802.11n, 802.11s, 802.11w).

IEEE 802.16. A body of standards established by the IEEE to facilitate point-to-multipoint broadband wireless transmission. The 802.16 body of standards is comprised of multiple sub groups (e.g., a/b/c/d/e/f/g/k/m) that supports line-of-sight, non-line-of-sight, and quality of service. It operates in the 2-11 GHz spectrum.

information assurance. Defined in DoDD 8500.01E (Reference (ad)).

interoperability. Defined in Reference (m).

minimal impact WLAN system. A system with minimal connectivity, information, and security requirements that is connected to the DoD Enterprise. These systems have a small number of users and a limited ability to transmit, store, or process DoD information, and therefore have a low level of risk associated with their confidentiality, integrity, and availability.

net-readiness. A concept that ensures that the most efficient technology is utilized in order to meet the needs of users, and that the system is capable of performing the missions or functions for which it is organized or designed to carry out.

non-IEEE 802.11. Any wireless transmission emanating from an RF device that is not based on the IEEE 802.11 body of standards. These transmissions can cause interference with IEEE 802.11 devices or may be difficult to monitor and/or detect with a WIDS. There are three categories of non-IEEE devices: IEEE 802.11 devices that operate in a non-standard frequency band; non-IEEE 802.11 devices that operate in the standard IEEE 802.11 frequency band; and non-IEEE 802.11 devices that operate in a non-standard frequency band. Common examples of non-IEEE 802.11 devices that cause interference with IEEE 802.11 devices include microwave ovens, cordless phones, and wireless webcams. Common examples of non-IEEE 802.11 devices that are difficult to monitor with a WIDS include Type 1 proprietary WLAN products, WLAN devices that have had frequency modifications, and proprietary microwave systems.

non-standard security solution. A security solution that does not adhere to a set of guidelines (e.g., FIPS validated, NIST validated, CC, NSA Type-1 encryptors).

PED. Defined in Reference (f).

secure end-to-end communications. The process of securing communications between devices, networks, and users, by providing confidentiality over vulnerable links between the end-user device and the security border of a DoD network (and/or between two interconnected DoD user devices). WLANs need to have confidentiality protection of wireless air interfaces in order to ensure secure end-to-end communications.

strong authentication. A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have).

Type 1 product. Defined in Committee on National Security Systems Instruction No. 4009 (Reference (ae)).

WIDS. A commercial wireless technology that assists designated personnel with the monitoring of specific parts of the RF spectrum to identify unauthorized wireless transmissions and/or activities. A WIDS consists of: RF component(s) with an antenna and radio designed to collect specific wireless transmissions; an analysis component that distinguishes between authorized and unauthorized wireless transmissions; and a display component that acts as the user interface that reports findings to designated personnel. WIDS may not provide a sufficient amount of monitoring support for non-IEEE 802.11 transmissions. Non-IEEE 802.11 transmissions include, but are not limited to, other RF devices that transmit and receive in the standard IEEE 802.11 frequency bands (currently 2.4 GHz and 5.8 GHz) and transceivers that are similar to IEEE 802.11 but operate in non-standard frequency band.

WLAN. A network in which a mobile node can connect to a local area network using a wireless (radio frequency-based) connection that spans a small geographical area (a single radio typically covers up to 500 meters).

WLAN-enabled PED. A PED that has been enabled to provide IEEE 802.11 communications. Examples of WLAN-enabled PEDs include, but are not limited to, personal digital assistants, cellular or personal communications system phones, Smartphones, e-mail devices, handheld audio/video recording devices, handheld devices, tablet computers, and laptop computers.

X.500. A series of International Telecommunication Union Telecommunication Standardization Sector standards for electronic directory services.