DoD INSTRUCTION 8420.01

COMMERCIAL WIRELESS LOCAL-AREA NETWORK (WLAN) DEVICES, SYSTEMS, AND TECHNOLOGIES

Originating Component: Office of the Chief Information Officer of the Department of Defense

Effective: November 3, 2017

Releasability: Cleared for public release. Available on the Directives Division Website at http://www.whs.esd.mil/DD/.

Reissues and Cancels: DoD Instruction 8420.01, "Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies," November 3, 2009

Approved by: John A. Zangardi, Acting Department of Defense Chief Information Officer

Purpose: This issuance:

- Establishes policy, assigns responsibilities, and provides procedures for the use of commercial WLAN devices, systems, and technologies in accordance with the authority in DoD Directive (DoDD) 5144.02.

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

- Clarifies use of non-DoD WLAN systems.

- Provides guidance on establishing a wireless network intrusion detection and prevention capability for monitoring WLAN and configuring it for improved event handling.

- Promotes reciprocity by requiring all DoD owned and operated unclassified WLANs to support access by authorized DoD users with a DoD provided WLAN-enabled PED.

- Provides guidance on the use of personal devices on a WLAN.

- Directs DoD Components to include support for unclassified WLAN systems in new DoD facilities during the planning stage to accommodate new technologies.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. 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 DoD (referred to collectively in this issuance 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 802.11-2016 and ratified amendments and revisions, that are used to store, process, receive, or transmit unclassified and classified information, which will be referred to as “IEEE 802.11.” This also includes the International Organization for Standardization (ISO)/International Electrotechnical Commission 8802-11: 2012 and ratified amendments and revisions for the international operational environment.

(3) 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) are not exempt from this issuance, except as noted in Paragraph 3.13. A PED that is capable of IEEE 802.11 connectivity will hereafter be referred to as a WLAN-enabled PED.

b. Does not apply to:

(1) Other wireless or cellular technologies.

(2) The detection segment of a PED, in accordance with DoDD 8100.02.

(3) The use of other wired or wireless access technologies or services on the WLAN-enabled PED or workstation that is not compliant with IEEE 802.11.

c. Nothing in this issuance alters or supersedes the existing authorities and policies of the Under Secretary of Defense for Intelligence (USD(I)) regarding the protection of sensitive compartmented information and sensitive compartmented information facilities (SCIF), as directed by Executive Order 12333 and other laws and regulations.

d. Nothing in this issuance alters or supersedes the existing authorities and policies of the USD(I) regarding the protection of special access program information and facilities.

1.2. POLICY. It is DoD policy that:

a. Unclassified WLAN systems must be standards-based and IEEE 802.11 compliant in accordance with Paragraph 3.1.a. of this issuance, employ certified radio frequency (RF) communications functions for interoperability in accordance with Paragraph 3.1.b., and employ certified or validated information assurance (IA) and cryptographic functions in accordance with Paragraph 3.2.

b. Unclassified WLAN-enabled PEDs and workstations must use antivirus software, personal firewalls, data-at-rest encryption, and implement authentication to access the device and the network, as applicable, in accordance with Paragraphs 3.2. and 3.3. of this issuance.

c. DoD Components are responsible for ensuring external WLAN systems that are not DoD owned or used by DoD employees or contractors, to include WLANs that are provided by commercial entities (e.g., hotspots), not-for-profit entities, federal partners, or research, development, test and evaluation environments, employ standards and controls commensurate with Paragraphs 1.2.a. and 1.2.b., where practical, in accordance with Paragraph 3.4. of this issuance.

d. Unclassified WLAN systems must provide guest access to authorized government and contractor users with a WLAN-enabled PED in accordance with Paragraph 3.5. of this issuance.

e. Unclassified WLAN systems and DoD WLAN-enabled PEDs and workstations may operate in spaces that are accredited collateral classified when authorized with written approval from the authorizing official (AO) in consultation with the Cognizant Security Authority Certified TEMPEST Technical Authority (CTTA), in accordance with DoDD 8100.02 and Paragraph 3.6. of this issuance.

f. Unclassified WLAN systems and associated security measures must be included in new DoD facilities during the planning stage in accordance with Paragraph 3.7. of this issuance.

g. Classified WLAN systems must be standards-based and IEEE 802.11 compliant, employ certified RF communications functions for interoperability, and employ certified or validated IA and cryptographic functions in accordance with Paragraphs 3.1. and 3.8. of this issuance. Classified WLAN systems must:

(1) Employ National Security Agency (NSA)-approved encryption end-to-end, and be protected with strong physical security, in accordance with Paragraphs 3.8.a. and 3.8.b. of this issuance.

(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, in accordance with Paragraph 3.8.c. of this issuance.

h. Classified WLAN-enabled PEDs must use NSA-approved encryption to protect classified data-in-transit and data-at-rest on PEDs in accordance with Paragraph 3.8. of this issuance.

i. Unclassified and classified DoD wired and wireless LANs must have a wireless intrusion detection system (WIDS) capability that can be used to monitor WLAN activity and identify WLAN-related policy violations in accordance with Paragraph 3.9. In addition, unclassified and classified DoD wired and wireless LANs must have a wireless intrusion prevention system (WIPS) capability to stop suspicious activity. Wireless intrusion prevention capabilities must not impact the performance of wireless intrusion detection capabilities (e.g., utilization factor).

1.3. INFORMATION COLLECTIONS.

a. DD Form 1494, "Application for Equipment Frequency Allocation," referred to in Paragraph 3.11. of this issuance, has been assigned Office of Management and Budget control number 0704-0188 and is prescribed in DoD Instruction (DoDI) 4630.09. The expiration date of this information collection is listed in the DoD Information Collections System at https://eitsdext.osd.mil/sites/dodiic/Pages/default.aspx.

b. Interoperability Certification and DD Form 1494, referred to throughout this issuance, does not require licensing with a report control symbol in accordance with Paragraphs 9 and 10 of Volume 1 of DoD Manual 8910.01.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO). The DoD CIO:

a. Provides oversight and policy development for all DoD WLAN activities.

b. Coordinates with the Intelligence Community (IC) Chief Information Officer (CIO) through the DoD and IC Information Security Risk Management Committees, calling a Joint IC-DoD Information Security Risk Management Committee when necessary, to ensure proper protection of IC information in implementing this issuance.

c. Assesses WLAN system architectures. Coordinates these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) to ensure that the processes for acquisition of WLAN systems are clear and understandable, and in accordance with the requirements of DoDD 5000.01 and DoDI 5000.02.

d. Coordinates with the USD(I) on policies that provide for the security of information in a networked environment, including those for IA, to ensure they are consistent with the requirements of policy and guidance issued by the USD(I) and the Director of National Intelligence.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.6., the Director, DISA:

a. Provides a template for the development of incident response plans and standards for intrusion detection and intrusion prevention on DoD wired and wireless LANs.

b. Directs the Joint Interoperability Test Command (JITC) to perform interoperability testing and provide interoperability certification of non-standard wireless solutions deployed within DoD, in accordance with DoDI 8330.01. The results from an interoperability test may be used to issue an interoperability certification, if the test criteria and configuration satisfy established requirements.

c. In collaboration with the NSA, transition all security requirements guides (SRG) to DoD annexes and support the NSA in the development of DoD annexes. Transition development of any current or planned SRGs to the National Information Assurance Partnership (NIAP).

2.3. USD(I). The USD(I), as the DoD senior security official and the senior agency official and having responsibility for the management and oversight of the DoD Information Security Program in accordance with DoDD 5143.01 and DoDI 5200.01:

a. Develops, coordinates, and oversees the implementation of a DoD Information Security Program regarding the possession and use of PEDs in DoD owned or controlled spaces processing or storing federal information to include controlled unclassified and classified information and activities.

b. Approves, as appropriate, requests for exceptions and waivers to the DoD Information Security Program policies and procedures pursuant to DoDI 5200.01.

2.4. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in Paragraph 2.6., the Director, DIA:

a. Provides intelligence support and guidance to DoD on the use of WLAN technologies.

b. Pursuant to DoDI 5200.01, administers DoD secure compartmented information security policies and procedures regarding wireless technologies for DIA-accredited SCIFs.

2.5. DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE (NSA/CSS). Under the authority, direction, and control of the USD(I), in addition to the responsibilities in Paragraph 2.6., and in accordance with National Security Directive 42, the Director, NSA/CSS:

a. Develops protection profiles for WLAN client systems, WLAN access systems, personal firewalls, antivirus protection packages, and WIDS/WIPS.

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

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

d. Serves 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, coordinates these activities with the Assistant Secretary of Defense for Research and Engineering.

e. Functions as the approval authority for certification of commercial classified WLAN products, in accordance with CNSS Policy No. 11 and DoDI 8500.01.

2.6. DOD COMPONENT HEADS. The DoD Component heads:

a. Direct that all acquisition of commercial WLAN products and subsequent operations comply with this issuance.

b. Promote joint interoperability through the adoption of commercial, standards-based, IA-certified WLAN products and provision for guest access in accordance with the requirements of this issuance.

c. Develop and provide, in conjunction with Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber, architectures, system requirements, and specifications to support WLAN solution interoperability and net-readiness testing.

d. Develop and provide architectures, specifications, systems engineering, and integration guidelines for command and control capable WLAN systems in coordination with NSA/CSS, in accordance with National Security Directive 42, to support WLAN solution interoperability and net-readiness testing.

e. 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.

f. Integrate WLAN intrusion detection and prevention with network management systems, configure them for effective event handling, and prepare and execute incident response plans for WLAN intrusion detection and prevention events.

g. Require all authorized users, privileged users, and IA managers of WLAN devices, systems, and technologies to receive IA awareness training and are trained and certified to perform respective IA duties, in accordance with DoDD 8100.02 and DoDD 8140.01.

h. Incorporate WLAN systems in procedures for physical security planning, construction, and acquisition of facilities or buildings and include unclassified WLAN systems in new DoD facilities during the planning stage as appropriate and in accordance with the guidance in the May 29, 2002 USD(AT&L) Memorandum.

i. Require that technical surveillance countermeasure practitioners, in accordance with DoDI 5240.05, and CTTA personnel are included in the planning, design, acquisition, deployment, and use of WLAN devices, systems, and technologies used within or in close proximity to SCIFs or accredited collateral classified spaces processing controlled unclassified or classified information.

SECTION 3: PROCEDURES

3.1. INDUSTRY STANDARDS COMPLIANCE FOR WLANS.

a. Standards-Based WLAN Technologies. DoD Components must require that only standards-based WLAN technologies are deployed for WLANs by adhering to:

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

(2) Internet Engineering Task Force (IETF) Standards. Only standards-based WLAN authentication between WLAN devices and WLAN infrastructure that is in compliance with the IETF Extensible Authentication Protocol (EAP) request for comment (RFC) 4017 standard must be used. The IETF EAP-Transport Layer Security RFC 5216 standard must be used as the only approved EAP method.

b. WLAN System Interoperability. DoD Components must require systems interoperability for WLANs by adhering to:

(1) Wireless Fidelity (Wi-Fi) Alliance Certification. All acquisitions of WLAN-enabled devices must be Wi-Fi and Wi-Fi protected access 2 (WPA2) Enterprise certified by the Wi-Fi alliance. WLAN-enabled devices that store, process, or transmit DoD information must be:

(a) Wi-Fi alliance certified as 802.11 physical-layer standards for device data communications interoperability. The Wi-Fi alliance certifies that WLAN-enabled devices are able to negotiate physical-layer and medium access control (MAC)-layer specification data communications and can establish International Standardization Organization (ISO) open systems interconnect 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 message authentication code protocol (known collectively as AES-CCMP) are able to negotiate medium access control-layer specification security communications and can establish an ISO open systems interconnect layer 2 security connection.

(2) JITC Approval. DoD Components must require systems meet overall end-to-end interoperability requirements as approved by the Joint Interoperability Testing Center (JITC), in accordance with National Security Directive 42. Obtaining Wi-Fi and WPA2 interoperability certifications does not eliminate the requirement for obtaining JITC certification for non-standard wireless solutions, in accordance with National Security Directive 42 and DoDI 8330.01.

3.2. UNCLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION.

DoD Components must use unclassified WLAN products that are certified and validated for secure end-to-end communications. In accordance with DoDI 8510.01, DoD Components must require that the system is appropriately categorized, assessed, and authorized by an AO.

a. National Institute of Standards and Technology (NIST) Certifications. In accordance with DoDD 8100.02, encryption of unclassified data-in-transit by WLAN-enabled PEDs, systems, and technologies must be implemented in a manner that protects the data end-to-end. All system components within a WLAN that wirelessly transmit unclassified DoD information must have cryptographic functionality that is validated under the NIST Cryptographic Module Validation Program (CMVP), as meeting requirements in accordance with Federal Information Processing Standards (FIPS) Publication 140. There are multiple FIPS 140 publications which hereafter will be referred to collectively as "FIPS 140." Encryption of data-at-rest that is validated under the NIST CMVP as meeting FIPS 140 must be implemented on WLAN-enabled PEDs, in accordance with DoDD 8100.02.

(1) WLAN-Enabled PEDs and Workstations. Unclassified WLAN-enabled PEDs and workstations must 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 and workstations may implement encryption either in software (via the WLAN supplicant) or in hardware (via the WLAN network interface card (NIC)).

(a) Software-Based Encryption. WLAN client supplicants supporting this configuration must disable, or otherwise preempt, the encryption capabilities of the WLAN client's NIC so the encryption can be performed solely by the supplicant software. WLAN client supplicants must implement the AES-CCMP for encryption as defined in IEEE Standard 802.11. The AES-CCMP encryption must be validated under the NIST CMVP as meeting FIPS 140.

(b) Hardware-Based Encryption. WLAN client NICs supporting this configuration must implement AES-CCMP as defined in IEEE Standard 802.11 within NIC hardware. The AES-CCMP encryption must be validated under the NIST CMVP as meeting FIPS 140.

(2) Access Point (AP)/WLAN Controller. Unclassified WLAN infrastructure devices must 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 must implement AES-CCMP as defined in IEEE Standard 802.11. The AES-CCMP encryption must be validated under the NIST CMVP as meeting FIPS 140.

(3) Data-at-Rest. Data-at-rest encryption must be implemented in a manner that protects unclassified information stored on WLAN-enabled PEDs by requiring the PED be powered on and credentials successfully authenticated in order for the data to be deciphered.

(a) Credentials for authenticating to data-at-rest protection must be public key infrastructure (PKI) certificates on the common access card (CAC), derived PKI certificates, or username and password for devices that cannot interface with the CAC, in accordance with DoDI 8520.02.

(b) Data-at-rest encryption must 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).

(c) In the event that a PED is lost or stolen, encryption must 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.

(d) All unclassified DoD data-at-rest on WLAN-enabled PEDs that is not approved for public release must be encrypted, in accordance with DoDI 8500.01.

(4) WLAN Authentication. Unclassified WLAN systems must have NIST CMVP FIPS 140 validated authentication schemes. DoD PKI authentication of users must be performed before users are granted access to DoD resources.

(a) WLAN Client Supplicant Authentication. Authentication must 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, secure hash standard) implemented during the EAP authentication process must be validated under the NIST CMVP as meeting FIPS 140.

(b) Authentication Server. Authentication servers are responsible for authenticating user or device credentials during EAP authentication; some also transmit the keying information that enables the AES-CCMP 4-way handshake as defined in IEEE Standard 802.11. 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 services, domain controllers, local user databases, and other authentication sources. The authentication server must transmit the keying information to the AP via a separate process.

1. EAP-Authentication. DoD Components that implement authentication servers that generate keying information and implement EAP-authentication of credentials provided by WLAN client supplicants must implement approved algorithms (e.g., hash message authentication code, secure hash standard , random number generator, AES, and Rivest-Shamir-Adleman) 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 before transmission to APs may validate the key wrapping under the NIST CMVP as meeting FIPS 140. The key wrapping must 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 or theft. If installed in unprotected environments, APs that store plaintext cryptographic keying information must be protected with added physical security to mitigate risks.

(a) 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; or

(b) DoD Components may physically secure APs by placing them inside of securely mounted, pick-resistant, lockable enclosures.

b. NIAP Validation. Any IA-enabled unclassified WLAN product must be NIAP common criteria (CC) validated, in accordance with CNSS Policy No. 11. WLAN-enabled solutions must be validated under the NIAP CC as meeting applicable U.S. Government (USG) approved WLAN protection profiles (e.g., WLAN client or WLAN access system), in accordance with the categorization of the system, as defined in DoDI 8500.01.

(1) WLAN Access Systems and Client Systems. WLAN-enabled PEDs and infrastructure must be NIAP CC validated. WLAN devices and infrastructure must be validated under the NIAP CC as meeting applicable USG approved WLAN access systems or client systems protection profiles. When a logical boundary is employed, WLAN controllers with integrated firewalls must be validated as meeting the USG approved firewall protection profile.

(2) Authentication Server. Authentication servers must be validated under the NIAP CC as meeting the USG approved authentication server protection profile.

(3) Antivirus. WLAN-enabled PEDs must use antivirus software when data services are used on those devices, as applicable, in accordance with DoDI 8500.01. Antivirus software must be validated as meeting applicable USG approved protection profiles under the NIAP.

(4) Personal Firewall. WLAN-enabled PEDs must use personal firewalls, as applicable, per DoDI 8500.01. Personal firewalls must be validated as meeting applicable USG approved protection profiles under the NIAP.

(5) WIDS/WIPS. DoD Components must use WIDS to actively screen for unauthorized WLAN activity for DoD wired and wireless LANs, in accordance with DoDD 8100.02. DoD Components may use WIPS to stop suspicious WLAN activity for DoD wired and wireless LANs. WIDS/WIPS must be validated under the NIAP CC as meeting the USG approved WIDS/WIPS protection profile.

3.3. UNCLASSIFIED WLAN AUTHENTICATION APPROACHES.

Authentication must be implemented at network and device levels as a method of protecting access to unclassified WLANs, in accordance with DoDD 8100.02.

a. DoD Components must use standards-based EAP authentication to authenticate unclassified WLAN users or devices. Unclassified WLAN-enabled PEDs and workstations used to access DoD PKI-enabled enterprise services (e.g., e-mail) must support DoD PKI for authentication, signing, and encrypting, as required, in accordance with DoDI 8520.02.

b. Unclassified WLAN devices, systems, and technologies must use authentication at the device and network levels in accordance with DoDD 8100.02.

(1) When “something you have” is used as one of the authentication factors, the authentication factor may include, but is not limited to:

(a) Key fobs.

(b) Smartcards.

(c) Universal serial bus tokens.

(d) Hardware tokens.

(e) Derived credentials.

(2) Unclassified WLAN-enabled commercial mobile devices (CMD) may employ DoD PKI credentials derived from CAC credentials and NIAP-validated key stores, in accordance with DoDI 8520.02. Authentication at the device and network levels may be achieved by assessing the combined processes of WLAN authentication and domain authentication.

c. DoD Components must implement unclassified WLAN systems with standards-based authentication mechanisms.

(1) WLAN authentication is achieved by establishing interoperability and validated secure implementations.

(2) WLAN authentication must implement the AES-CCMP 4-way handshake key exchange as defined in IEEE Standard 802.11.

(3) WLAN devices and infrastructure must be WPA2 Enterprise certified to ensure authentication can be negotiated in a mixed vendor WLAN system implementation.

(4) Where WPA2 Enterprise is employed, WLAN infrastructure must implement 802.1X access control to prevent WLAN access to unauthorized WLAN devices and enforce authentication of authorized WLAN devices, before providing access.

(5) EAP authentication must facilitate the verification of credentials provided by authorized WLAN devices or users.

(6) Cryptographic modules implemented to facilitate authentication must be FIPS 140 validated in accordance with Paragraph 3.2. of this issuance.

3.4. NON-DOD UNCLASSIFIED WLAN SYSTEMS. DoD Components must require DoD employees or contractors using external WLAN systems that are not DoD owned or operated, to include WLANs that are provided by commercial entities (e.g., hotspots), not-for-profit entities, federal partners, or research, development, test and evaluation environments, employ standards compliant with Paragraph 3.1., and controls validated in accordance with Paragraph 3.2., as practical. When connected via a non-DoD WLAN, users must immediately establish a connection to the DoD network via an approved method (e.g., virtual private network, transport layer security).

a. Industry Standards Compliance. Users of non-DoD WLAN systems must employ the standards-based WLAN technologies of Paragraph 3.1.a. and comply with the interoperability certifications of Paragraph 3.1.b.(1).

(1) Where WPA2 Enterprise is not available, users of non-DoD WLAN systems must employ WPA2 Personal (also known as WPA2 Pre-Shared Key) or Passpoint with AES encryption certified by the Wi-Fi alliance for device security communications interoperability. If users cannot employ WPA2, they should not use the external WLAN system.

(2) JITC approval as stated in Paragraph 3.1.b.(2) is desired where practical.

b. Security Certification and Validation.

(1) Users of non-DoD WLAN systems must employ the controls of Paragraph 3.2.a. in NIST-validated mode, as practical.

(2) NIAP validation per Paragraph 3.2.b. is desired where practical.

(3) Users of non-DoD WLAN systems must employ controls in accordance with DoDI 8500.01, DoDI 1035.01, and the Remote Access Policy Security Technical Implementation Guide (STIG) for telework and remote access and in accordance with DoDI 8582.01. If users cannot employ controls, they should not use the external WLAN system.

(4) Unclassified WLAN devices must be protected in accordance with their respective DoD Component's policies and procedures.

3.5. GUEST ACCESS FOR UNCLASSIFIED WLAN SYSTEMS.

a. DoD Components must require unclassified WLANs provide guest access to authorized government and contractor users with a DoD WLAN-enabled PED in accordance with the Network Infrastructure Policy, Joint Information Environment Enterprise Remote Access, and Remote Access Policy STIGs.

b. Unclassified WLAN systems may provide guest access to authorized government and contractor users with a non-DoD WLAN-enabled PED in accordance with the STIGs.

c. Guest traffic must be segmented by a physical boundary or a logical boundary with additional controls (e.g., spectrum sweeps). The cognizant AO must determine if guest users must be sponsored by host organizations. Guest users may access DoD resources via a virtual private network in accordance with the Remote Access Policy STIG. Unclassified WLAN systems that provide guest access are prohibited from sharing infrastructure with classified networks. Unclassified WLANs with guest access must comply with industry standards, security certification and validation, and authentication of Paragraphs 3.1., 3.2., and 3.3.

3.6. UNCLASSIFIED WLAN IN ACCREDITED COLLATERAL CLASSIFIED SPACES. DoD Components may operate unclassified WLAN systems and DoD WLAN-enabled PEDs and workstations in spaces that are accredited collateral classified in accordance with the Network Infrastructure Policy, Mobile Policy, and CMD Policy STIGs, and Paragraph 3.10. and in coordination with the senior agency official. RF transmitter separation must be at least 1 meter away from equipment processing classified information that are within spaces accredited for collateral classified in accordance with CNSS Advisory Memorandum TEMPEST/1-13. Unclassified WLANs in accredited collateral classified spaces must comply with industry standards, security certification and validation, and authentication of Paragraphs 3.1., 3.2., and 3.3. and meet technical surveillance countermeasure requirements.

3.7. UNCLASSIFIED WLAN IN NEW FACILITIES. DoD Components must include unclassified WLAN systems and associated security measures in new DoD facilities during the planning stage in accordance with the May 29, 2002 USD(AT&L) Memorandum, which provides protective design planning, construction, sustainment, restoration, and modernization criteria for facilities. New WLAN technologies may require infrastructure improvements (e.g., power, cabling, distributed antenna systems).

3.8. CLASSIFIED WLAN SECURITY CERTIFICATION AND VALIDATION. DoD Components must ensure that classified WLAN products are approved by the NSA Commercial Solutions for Classified (CSfC) Program in accordance with CNSS Policy No. 7. Classified WLAN systems use two layers of protection in accordance with the CSfC Campus WLAN capability package (CP) or mobile access CP (MACP). Per DoDI 8510.01, DoD Components must require that the system is appropriately categorized and authorized by an AO. DoD Components must require that management of the implementation and use of classified WLAN-enabled PEDs is performed in accordance with the guidance in the September 25, 2015 OSD Memorandum.

a. Certification of Classified WLAN Products. Classified WLAN solutions must be approved by NSA as:

(1) CSfC, in accordance with the Campus WLAN CP, MACP, and associated risk assessments, registered through the CSfC Program, and NIAP CC validated, in accordance with CNSS Policy No. 11 and DoDI 8500.01;

(2) Tailored, by working with NSA and obtaining a National Manager letter of approval; or;

(3) Government off the shelf, as authorized to process and protect classified information sent and received over commercial infrastructure.

b. Physical Security of Classified WLANs.

(1) WLAN APs used to transmit or process classified information must be physically secured. Methods must exist to facilitate the detection of tampering. WLAN APs must have controlled physical security, in accordance with Volumes 3 and 4 of DoD Manual 5200.01.

(2) Physical or electronic inventories may be conducted by polling the serial number or MAC address. APs not stored in a communication security approved security container must be physically inventoried.

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

c. IA for Classified WLANs. Implementation of classified WLAN devices, systems, and technologies must:

(1) Be rekeyed in accordance with the CSfC Campus WLAN CP or MACP.

(2) Use a session timeout capability in accordance with the CSfC Campus WLAN CP or MACP.

(3) Employ authentication measures for the WLAN-enabled PED and WLAN, in accordance with CNSS Policy No. 22. Classified WLAN-enabled PEDs and workstations used to access DoD PKI-enabled enterprise services (e.g., e-mail) must support DoD PKI for authentication, signing, and encrypting, as required, in accordance with DoDI 8520.02.

(4) Include integrity and non-repudiation controls.

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

(6) Require a SIPRNET connection approval package is on file with the SIPRNET Connection Approval Office and current to include the classified WLAN system.

(7) Be permitted in a U.S. permanent, temporary, or mobile SCIF if approved in accordance with IC Directive Number 705, IC Directive Number 503, or DIA SCIF policy requirements.

(8) Require that the CTTA is notified before installation and operation of WLANs intended for use in processing or transmitting classified information, in accordance with CNSS Advisory Memorandum TEMPEST/1-13.

(9) Require that all WLAN systems are categorized and authorized, in accordance with DoDI 8510.01 and CNSS Policy No. 22.

(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 must be protected by:

(1) Implementing encryption of classified data-at-rest with NSA-certified encryption at a level consistent with the classification of the data stored on the device in accordance with the CSfC Campus WLAN CP, MACP, or Data at Rest CP;

(2) Removing storage media that contains classified information from the PED and storing it within the appropriate General Services Administration-approved security container, in accordance with Volume 3 of DoD Manual 5200.01, or

(3) Placing the entire PED within the appropriate Government Services Administration-approved security container, in accordance with Volume 3 of DoD Manual 5200.01.

e. Government Private Wi-Fi (or Wireless) Networks, as defined in the NSA Commercial Solutions for Classified Programs (CSfC) Mobile Access Capability Package, are accredited as Unclassified WLANs unless specifically accredited to carry unencrypted Classified data.

3.9. WLAN INSTRUSION DETECTION AND PREVENTION. DoD Components must ensure a WIDS/WIPS 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 in accordance with the CSfC Campus WLAN CP, Intrusion Detection and Prevention System SRG, Network Infrastructure Policy STIG, and Paragraph 3.10. DoD Components must implement WIPS to stop suspicious activity on unclassified and classified DoD wired and wireless LANs in accordance with the CSfC Campus WLAN CP, Intrusion Detection and Prevention System SRG, Network Infrastructure Policy STIG, and Paragraph 3.10. DoD Components must develop and execute incident response plans for WIDS/WIPS events. DoD Components must ensure that WIPS does not impact the performance of WIDS (e.g., utilization factor).

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

b. WIDS/WIPS Implementation Criteria. The WIDS/WIPS must continuously scan for and detect authorized and unauthorized WLAN activities 24 hours a day, 7 days a week. Scanning must include a location-sensing capability that enables designated personnel to locate, identify, and take appropriate actions to mitigate IEEE 802.11 threats. The WIDS/WIPS must be integrated with network management systems and configured for effective event handling in accordance with DoDI 8410.03.

3.10. DOD ANNEX, SRG, AND STIG COMPLIANCE. In addition to adhering to the procedures specified in this section, incorporate the security best practices specified in the Network Infrastructure Policy, Network WLAN, CMD Policy, and applicable operating system STIGs, and other applicable SRGs and STIGs**,** as they pertain to the implementation of WLANs. NSA and DISA are transitioning SRGs to DoD annexes of NIAP protection profiles. DoD Components must comply with applicable NIAP protection profiles and DoD annexes. If NIAP protection profiles and DoD Annexes are not published, compliance with SRGs is acceptable.

3.11. WLAN SPECTRUM SUPPORTABILITY.

a. Require spectrum supportability before acquiring spectrum-dependent WLAN systems in accordance with DoDI 4650.01.

b. Require compliance with the DoD Electromagnetic Environmental Effects Program in accordance with DoDI 3222.03.

c. Require 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 464C.

d. DoD requires non-licensed devices operating in the United States and its possessions must be registered with the local spectrum management office.

(1) Outside the United States and its possessions, each theater commander and host nation must determine if frequency support is available and authorized.

(2) 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 United States and its possessions. After obtaining favorable host nation guidance, users may request frequency assignment, as needed.

3.12. 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 will be subject to review and assessment by the 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.

3.13. EXCEPTIONS TO WLAN DEVICES, SYSTEMS, OR TECHNOLOGIES.

a. Unclassified WLAN Security Exceptions. AOs are authorized to grant exceptions to the use of unclassified WLAN devices, systems, or technologies.

(1) Non-Compliant WLAN Devices, Systems, or Technology Exceptions. Exceptions may be made by the AO 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 Risk Management Framework authorization package, in accordance with DoDI 8510.01. The documentation must 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 DoD Information Network (DoDIN). AOs must review the Risk Management Framework authorization package to make an informed decision about the impact to interoperability before granting an exception.

(a) Exceptions for the Use of NSA-Certified Devices on Unclassified WLANs. Use of NSA-certified products is also acceptable for unclassified data, when operating in the secure mode. NSA-certified WLAN products other than CSfC-compliant 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 AO for minimal impact WLANs systems. These systems must be segmented from the DoDIN via a wireless demilitarized zone that provides network intrusion detection and prevention capabilities and limits ports and protocols to the minimum set necessary to achieve mission objectives. A STIG-compliant firewall must be located at the system's point of entry onto the DoDIN.

(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 issuance. DoD Components must protect backhaul data-in-transit with FIPS 140 validated encryption modules in accordance with DoDD 8100.02.

(3) Unclassified WIDS/WIPS Exceptions. Exceptions to WIDS/WIPS implementation criteria stated in this issuance may be made by the AO for DoD wired and WLANs operating environments. This exception allows the AO 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 3.9.b. 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/WIPS unless noted in accordance with Paragraph 3.8.a.

GLOSSARY

G.1. ACRONYMS.

AES	advanced encryption standard
AES-CCMP	advanced encryption standard-counter with cipher block chaining message authentication code protocol
AO	authorizing official
AP	access point
CAC	common access card
CC	common criteria
CIO	chief information officer
CMD	commercial mobile device
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CP	capability package
CSfC	Commercial Solutions for Classified
CTTA	Certified TEMPEST Technical Authority
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDIN	DoD information network
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standards
IA	information assurance
IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Standards Organization

JITC	Joint Interoperability Test Command
LAN	local area network
MAC	medium access control
MACP	mobile access capability package
MIL-STD	military standard
NIAP	National Information Assurance Partnership
NIC	network interface card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
PED	portable electronic device
PKI	public key infrastructure
RF	radio frequency
RFC	request for comments
SCIF	sensitive compartmented information facility
SIPRNET	SECRET Internet Protocol Router Network
SRG	security requirements guide
STIG	security technical implementation guide
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. Government
Wi-Fi	wireless fidelity
WIDS	wireless intrusion detection system
WIPS	wireless intrusion prevention system
WLAN	wireless local area network
WPA2	Wi-Fi Protected Access 2

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

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

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

authentication server. Infrastructure to perform authentication functions as defined in CNSS Instruction No. 4009. IEEE Standard 802.11 includes Remote Authentication Dial In User Service (RADIUS) (IETF RFC 5080) as an authentication server, which is part of a WLAN system. 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 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 (International Electrotechnical Commission 8802-11: 2012 calls the keying information the "authentication, authorization, and accounting key"). 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.

cellular technology generations (G). 2.5G, 3G, 4G and 5G/Long Term Evolution cellular systems.

CMD. A subset of PEDs that provide one or more commercial wireless interfaces along with a compact user input interface (e.g., Touch Screen, Miniature Keyboard) and exclude PEDs running a multi-user operating system (e.g., Windows, Mac). This includes, but is not limited to smart phones, tablets, and e-readers.

detection segment of a PED. The laser used in optical storage media; between a barcode and a scanner head; or RF energy between RF identification tags, both active and passive, and the reader/interrogator.

guest access. Includes but is not limited to non-organization, assigned DoD personnel and contractors, volunteers, and non-federal-entity personnel authorized to support DoD missions and activities; other international, federal, State, local, or tribal government personnel supporting DoD missions and activities; and other U.S. civilian persons on approved official business in DoD facilities. Some environments may allow non-official business (e.g., morale, welfare, and recreation) or public visitors (e.g., hospitals).

IA. Defined in CNSS Instruction No. 4009.

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, 3.6, 4.9/5, and 60 gigahertz spectrum bands in order to provide communication in WLAN environments. The family of standards is comprised of the IEEE Standard 802.11-2016 (which incorporates 802.11a/b/d/e/g/h/i/j/k/n/p/r/s/u/v/w/y/z), a number of amendments (e.g., 802.11ac, 802.11ad, 802.11af), and revisions.

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 gigahertz spectrum.

interoperability. Defined in DoDI 8330.01.

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. Minimal impact WLANs systems are systems that: do not provide connectivity to WLAN-enabled PEDs or workstations (e.g., backhaul systems); have no available FIPS 140 validated, 802.1X, EAP-transport layer security supplicant; support a very small number of users for a specific mission (i.e., 10 or fewer users); are standalone networks; or are highly specialized WLAN systems that are isolated from the DoDIN (e.g., handheld personal digital assistants used as radio-frequency identification readers, a network of WLAN-enabled Voice over Internet Protocol phones).

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 or detect with a WIDS/WIPS. 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/WIPS include proprietary classified WLAN products, WLAN devices that have had frequency modifications, and proprietary microwave systems. Form factors may include memory cards, Personal Computer Memory Card International Association cards, ExpressCards, cellular network interface cards, or Universal Serial Bus adapters.

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

other wireless technologies. IEEE 802.15 wireless personal area network standards (e.g., Bluetooth, ultra-wideband, ZigBee), IEEE 802.16 wireless metropolitan area network standards (e.g., Worldwide Interoperability for Microwave Access systems, local multipoint distribution service), IEEE 802.20 mobile broadband wireless access standards, IEEE 802.22 wireless regional area network standards, proprietary microwave communications systems, receive-only pagers, global positioning system receivers, medical devices (e.g., hearing aids), and personal life support systems.

PED. Defined in DoDD 8100.02.

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, or between two interconnected DoD user devices. WLANs need to have confidentiality protection of wireless air interfaces in order to provide secure end-to-end communications.

WIDS/WIPS. A commercial wireless technology that assists designated personnel with the monitoring of specific parts of the RF spectrum to identify and stop unauthorized or suspicious wireless transmissions or activities. A WIDS/WIPS 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 or normal and suspicious wireless transmissions; and a display component that acts as the user interface that reports findings to designated personnel. WIPS deters attacks at network and application layers and does not defeat hardware, software, or RF at the physical layer. Some WIPS can terminate suspicious connections by sending messages through the air to deassociate sessions and refusing to permit new connections. Some WIPS can instruct a switch on the wired network to block network activity involving suspicious WLAN clients or APs. WIDS/WIPS 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, 3.6, 4.9/5.8, and 60 gigahertz) 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 LAN using a wireless (RF-based) connection that spans a small geographical area (a single radio typically covers up to 500 meters).

WLAN-enabled devices. NICs, APs, WLAN controllers, WLAN switches.

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 and video recording devices, handheld devices, tablet computers, and laptop computers and their supplicants.

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

REFERENCES

Committee on National Security Systems Advisory Memorandum TEMPEST/1-13, "RED/BLACK Installation Guidance," January 17, 2014

Committee on National Security Systems Policy No. 7, "Policy on the Use of Commercial Solutions to Protect National Security Systems," December 9, 2015

Committee on National Security Systems Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products," June 10, 2013

Committee on National Security Systems Policy No. 17, "Policy on Wireless Systems," January 2014

Committee on National Security Systems Policy No. 22, "Policy on Information Assurance Risk Management for National Security Systems," January 2012

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems Glossary," current edition

Commercial Solutions for Classified Campus Wireless Local Area Network Capability Package, current edition

Commercial Solutions for Classified Data at Rest Capability Package, current edition

Commercial Solutions for Classified Mobile Access Capability Package, current edition

Defense Information Systems Agency Commercial Mobile Device Policy Security Technical Implementation Guide, current edition

Defense Information Systems Agency CSfC WLAN Policy Security Technical Implementation Guide, current edition

Defense Information Systems Agency Harris SecNet 11/54 Security Technical Implementation Guide, current edition

Defense Information Systems Agency Intrusion Detection and Prevention System Security Requirements Guide, current edition

Defense Information Systems Agency Joint Information Environment Enterprise Remote Access Security Technical Implementation Guide, current edition

Defense Information Systems Agency Mobile Policy Security Technical Implementation Guide, current edition

Defense Information Systems Agency Network Infrastructure Policy Security Technical Implementation Guide, current edition

Defense Information Systems Agency Network WLAN Security Technical Implementation Guide, current edition

Defense Information Systems Agency Remote Access Policy Security Technical Implementation Guide, current edition

DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

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

DoD Directive 8140.01, “Cyberspace Workforce Management,” August 11, 2015, as amended

DoD Instruction 1035.01, “Telework Policy,” April 4, 2012

DoD Instruction 3222.03, “DoD Electromagnetic Environmental Effects (E3) Program,” August 25 2014, as amended

DoD Instruction 4630.09, “Wireless Communications Waveform Development and Standardization,” July 15, 2015, as amended

DoD Instruction 4650.01, “Policy and Procedures for Management and Use of the Electromagnetic Spectrum,” January 9, 2009, as amended

DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” January 7, 2015, as amended

DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),” April 21, 2016

DoD Instruction 5240.05, “Technical Surveillance Countermeasures (TSCM),” April 3, 2014

DoD Instruction 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” May 21, 2014

DoD Instruction 8410.03, “Network Management (NM),” August 29, 2012

DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014

DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, as amended

DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” May 24, 2011

DoD Instruction 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems,” June 6, 2012, as amended

DoD Manual 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” February 24, 2012, as amended

DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” February 24, 2012

DoD Manual 8910.01, Volume 1, “DoD Information Collections Manual: Procedures for DoD Internal Information Collections,” June 30, 2014, as amended

Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended

Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules,” May 25, 2001, as amended

Institute of Electrical and Electronics Engineers Standard 802.11-2016, “Institute of Electrical and Electronics Engineers 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," December 14, 2016[1]

Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008

Intelligence Community Directive Number 705, "Sensitive Compartmented Information Facilities," May 26, 2010

International Standards Organization/International Electrotechnical Commission 8802-11: 2012, "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," November 1, 2012[2]

Military Standard-461F, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," December 10, 2007

Military Standard-464C, "Electromagnetic Environmental Effects Requirements for Systems," December 1, 2010

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990[3]

Office of the Secretary of Defense Memorandum, "Security and Operational Guidance for Classified Portable Electronic Devices," September 25, 2015

Under Secretary of Defense, Acquisition, Technology and Logistics Memorandum, "Department of Defense Unified Facilities Criteria," May 29, 2002

[1] Copies may be obtained at http://ieeexplore.ieee.org/document/7786995/

[2] Copies may be purchased from the ISO website, 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