DoD Instruction 8420.01

Commercial Wireless Local-Area Network Devices, Systems, and Technologies

Originating Component:	Office of the DoD Chief Information Officer
Effective:	December 9, 2025
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8420.01, "Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies," November 3, 2017
Approved by:	Katherine Arrington, Performing the Duties of DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for the use of commercially procured, Institute of Electrical and Electronics Engineers (IEEE) 802.11 (referred to in this issuance as "IEEE 802.11") capable, wireless local-area network (WLAN) devices, systems, and technologies (i.e., wireless fidelity (Wi-Fi)) that are used to transmit, receive, process, or store unclassified and classified information.
- Establishes Wi-Fi Protected Access 3 (WPA3)-Enterprise using 192-bit mode, or latest Wi-Fi Alliance (WFA) version configured at minimum 192-bit mode, as the unclassified and classified DoD encryption standard for DoD WLAN systems, hereafter referred to as WPA3-Enterprise 192-bit mode.
- Specifies the minimum set of security measures required on DoD owned and operated WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store unclassified and classified information, including non-DoD owned approved mobile devices (AMD), hereafter referred to as a DoD WLAN-enabled PED.
- Clarifies use of non-DoD WLAN systems.
- Promotes reciprocity by requiring all DoD owned and operated unclassified WLANs to support access by authorized DoD employees (government and contractors), hereafter referred to as DoD users, with a DoD WLAN-enabled PED.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance:

a. Applies to:

(1) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of 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) DoD WLAN devices, systems, and technologies that:

(a) Are used to transmit, receive, process, or store unclassified and classified information in accordance with IEEE 802.11 and the International Organization for Standardization(ISO) or International Electrotechnical Commission 8802-11.

(b) Have direct or indirect connection to operational DoD networks (i.e., Nonclassified Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET)), except as noted in Paragraph 3.13.

b. Does not apply to:

(1) Other wireless technologies.

(2) The use of other wireless access technologies or services on WLAN-enabled PEDs that are not compliant with IEEE 802.11 (e.g., IEEE 802.15 Bluetooth, Zigbee).

1.2. POLICY.

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 DoD Instruction (DoDI) 8330.01, employ certified or validated cybersecurity (formerly information assurance (IA)) and cryptographic functions in accordance with Paragraph 3.2., and require spectrum supportability in accordance with Paragraph 3.11.

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

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

(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 cybersecurity measures that are consistent with Committee on National Security Systems (CNSS) Policy No. 17, in accordance with Paragraph 3.8.c.

c. Unclassified and classified DoD WLANs must have a wireless intrusion detection system (WIDS) capability used to monitor WLAN activity and identify WLAN related policy violations in accordance with Paragraph 3.9. In addition, unclassified and classified DoD WLANs, may have a wireless intrusion prevention system (WIPS) capability to stop suspicious activity, as determined by the authorizing official (AO) based on an assessment of vulnerabilities and risks. WIPS capabilities must not impact the performance of WIDS capabilities (e.g., utilization factor). DoD Component heads must consult with legal counsel and the Senior Component Official for Privacy (SCOP) to develop a common understanding of the legal (i.e., civil liberties) and privacy considerations related to the use of WIPS and the collection of data before implementation.

d. Devices with radiofrequency or over-air communications capabilities, including unclassified and classified DoD WLANs, are prohibited in sensitive compartmented information facilities (SCIFs) without an approved waiver obtained through the Under Secretary of Defense for Intelligence and Security (USD(I&S)) from the Intelligence Community Wireless Steering Committee in accordance with the January 19, 2017 Director of National Intelligence (DNI) Executive Correspondence.

e. Unclassified and classified WLANs may not both be deployed, present, or utilized in the same space without joint approval from the USD(I&S) and the DoD Chief Information Officer (DoD CIO).

f. Nothing in this issuance alters or supersedes the existing authorities and policies of the DNI or the USD(I&S), as the Senior Agency Official for Security, regarding the protection of sensitive compartmented information (SCI), SCIFs, and special access program (SAP) information and facilities as directed by Executive Order 12333, Executive Order 13526, and other laws and regulations.

SECTION 2: RESPONSIBILITIES

2.1. DOD CIO.

The DoD CIO:

a. Oversees 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, in accordance with DoDI 8510.01, to oversee proper protection of IC information in implementing this issuance.

c. Assesses WLAN system architectures and coordinates these activities with the Under Secretary of Defense for Acquisition and Sustainment to verify 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&S) on information security and cybersecurity policies, as appropriate, to align with the policy requirements and guidance issued by the DNI; directs policy for the Director, National Security Agency / Chief, Central Security Service (DIRNSA/CHCSS) as it relates to his/her duties as the National Manager for National Security Systems, regarding DoD network operations and cybersecurity matters.

e. In conjunction with the USD(I&S), approves DoD Component requests for both classified and unclassified WLANs to be deployed, present, or utilized in the same space.

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 2.7., the Director, DISA:

a. Provides a best practices template for the development of DoD Component incident response and contingency plans and standards for WIDS and WIPS on DoD WLANs.

b. Directs the Joint Interoperability Test Command (JITC) to perform interoperability testing and provide interoperability certification of non-standard WLAN solutions (i.e., does not adhere to guidelines in this issuance) 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. Develops and maintains a Network WLAN security technical implementation guide (STIG) for WLAN systems.

d. Coordinates with the DoD Component heads, as appropriate, to identify and propose information technology (IT) standards that support a capability-focused and architecture-based approach for achieving IT interoperability in accordance with DoDI 8310.01.

2.3. USD(I&S).

The USD(I&S), as the DoD senior security official and the senior agency official that has responsibility for the management and oversight of the DoD Information Security Program in accordance with DoDD 5143.01, DoDI 5200.01, DoDI 5200.48:

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.

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

c. Coordinates requests from DoD Components for waivers from the Intelligence Community Wireless Steering Committee for unclassified and classified DoD WLANs in SCIFs in accordance with the January 19, 2017 DNI Executive Correspondence.

d. In conjunction with the DoD CIO, approves DoD Component requests for both classified and unclassified WLANs to be deployed, present, or utilized in the same space.

2.4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

The Under Secretary of Defense for Acquisition and Sustainment oversees the Military Services' compliance with DoD acquisition guidance when acquiring, deploying, and sustaining DoD WLAN devices, systems, and technologies as defined in DoDD 5000.01, DoDI 5000.02, and this issuance.

2.5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA).

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.7., the Director, DIA:

a. Supports DoD with all-source intelligence reporting concerning the security and vulnerability of WLAN technologies.

b. Pursuant to DoDI 5200.01, administers SCI security policies and procedures regarding wireless technologies for DIA accredited SCIFs.

c. As the Defense Intelligence Enterprise manager for Joint Worldwide Intelligence Communications System (JWICS), develops policy and guidance regarding the acquisition and employment of commercial WLAN products and services connected to JWICS in compliance with this issuance, and consistent with DoDD 5105.21 and DoDI 8330.01.

d. Provides information and communications technology and operational technology cybersecurity supply chain risk management assessments on request for entities developing, integrating, or providing WLAN information and communications technology and operational technology products (e.g., hardware and software) and services that are responsive to DoD requirements.

2.6. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization of the NSA funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.7, the DIRNSA/CHCSS, in coordination with the DoD Chief Information Security Officer:

a. Develops protection profiles (PP) for WLAN client systems, WLAN access systems, WLAN firewalls, WIDS/WIPS, virtual private networks (VPNs), and, as determined by DoD CIO, cybersecurity products (e.g., firewalls, file integrity checkers, virus scanners, intrusion detection systems, anti-malware software) to meet DoD cybersecurity requirements in accordance with DoDI 8500.01.

b. Provides risk and vulnerability assessments on request 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, in coordination with DoD CIO, for WLAN cybersecurity technology research and development, to include protection mechanisms, detection and monitoring, response and recovery, and cybersecurity assessment tools and techniques. As necessary, coordinates these activities with the Under 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.

2.7. DOD COMPONENT HEADS.

The DoD Component heads:

a. Direct that all acquisition of commercial WLAN products and subsequent operations comply with this issuance and are consistent with DoDD 5000.01.

b. Promote joint interoperability through the adoption of commercial, standards-based, cybersecurity certified or validated WLAN products and provision for guest access in accordance with the requirements of this issuance and consistent with DoDI 8330.01.

c. Develop and provide, in conjunction with Joint Staff Directorate for Command, Control, Communications, and Computers or 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 consultation with DIRNSA/CHCSS, in accordance with National Security Directive 42 or any successor issuances, to support WLAN solution interoperability and net-readiness testing.

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

f. Integrate WIDS and WIPS (if employed), with network management systems, configure them for effective event handling, and prepare and execute incident response plans for WIDS/WIPS events. Consult with legal counsel and the SCOP to develop a common understanding of the legal (i.e., civil liberties) and privacy considerations related to the use of WIPS and the collection of data before implementation.

g. Require all authorized users receive cybersecurity awareness training pursuant to DoDI 8500.01 and all privileged users and cybersecurity managers of WLAN devices, systems, and technologies are trained and qualified to perform respective cybersecurity duties, in accordance with DoDD 8100.02 and DoDD 8140.01.

h. Incorporate WLAN systems in procedures for telecommunications infrastructure design, physical security planning, construction, and acquisition of facilities or buildings during the planning stage and, as determined by threat assessment, include unclassified WLAN systems in new unclassified DoD facilities, where NIPRNET access is required, during the planning stage in accordance with Unified Facilities Criteria 1-200-01 and guidance in the May 29, 2002 Under Secretary of Defense, Acquisition, Technology and Logistics Memorandum.

i. Require that technical surveillance countermeasure practitioners, in accordance with DoDI 5240.05, and Certified TEMPEST Technical Authority (CTTA) personnel, in accordance with CNSS Advisory Memorandum TEMPEST/1-13, are included in the planning, design, acquisition, deployment, and use (i.e., implementation and response procedures) of WLAN devices, systems, and technologies employed within or in close proximity to SCIFs or accredited collateral classified spaces (i.e., non-SCI and non-SAP).

j. All DoD owned and operated unclassified and classified WLAN systems must use Wi-Fi Protected Access 3 (WPA3)-Enterprise only mode until public key infrastructure (PKI) certificates are available to support WPA3-Enterprise 192-bit mode in accordance with the December 23, 2022 DoD CIO Memorandum and requirements in CNSS Policy No. 15 Annex B. These systems must then transition to WPA3-Enterprise 192-bit mode once required PKI certificates are available.

k. Provide DoD CIO with transition plans to WPA3 Enterprise only mode and then to WPA3 Enterprise 192-bit mode within 1 year from the publication of this instruction.

l. Use applicable IT standards, including data standards, that are prescribed by the DoD CIO in the DoD IT Standards Registry as mandated or emerging in accordance with DoDIs 8310.01 and 8330.01.

m. Incorporate operations security (OPSEC) considerations in all unclassified and classified DoD WLANs plans and procedures to protect critical or sensitive information that, if compromised, could negatively impact DoD operations or activities in accordance with DoDD 5205.02E.

n. Ensure records and information established and created in accordance with this issuance are retained in accordance with DoDI 5015.02 and DoD Component records management disposition schedules.

2.8. COMMANDANT, UNITED STATES COAST GUARD.

In addition to the responsibilities in Paragraph 2.7., the Commandant, United States Coast Guard adheres to DoD requirements, standards, and policies in this issuance in accordance with the January 19, 2017 Memorandum of Agreement between the Department of Defense and the Department of Homeland Security.

SECTION 3: PROCEDURES

3.1. INDUSTRY STANDARDS COMPLIANCE FOR WLANS.

a. Standards-based WLAN Technologies.

DoD Component heads 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 (TLS) RFC 5216 standard must be used as the only approved EAP method.

b. WLAN System Interoperability.

DoD Component heads must require systems interoperability for WLANs by adhering to:

(1) Wi-Fi WFA Certification.

All acquisitions of WLAN devices, systems, and technologies must be Wi-Fi and WPA3 Enterprise 192-bit mode or later version certified by the WFA. WLAN devices, systems, and technologies that transmit, receive, process, or store DoD information must be:

(a) WFA certified as IEEE 802.11 physical layer standards for device data communications interoperability. The WFA certifies that WLAN devices, systems, and technologies can negotiate physical layer and medium access control (MAC) layer specification data communications and can establish ISO open systems interconnect layer 1 and layer 2 connections.

(b) WPA3-Enterprise certified for device security communications interoperability. WPA3 Enterprise 192-bit mode or later version certifies that WLAN devices, systems, and technologies that implement Advanced Encryption Standard (AES) Galois or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (GCMP) can negotiate MAC layer specification security communications and can establish an ISO open system interconnect layer 2 security connection.

(2) JITC Approval.

DoD Component heads must require systems meet overall end to end interoperability requirements as approved by the Joint Staff J6 for joint systems or the DoD Component for non-joint systems in accordance with National Security Directive 42 or any successor issuances. Joint systems must be certified for joint interoperability by the JITC in accordance with DoDI 8330.01.

(3) DoD IT Standards.

Only WLAN systems compliant with DoD IT standards as prescribed in the DoD IT Standards Registry, as mandated or emerging in accordance with DoDI 8310.01 and DoDI 8330.01 must be acquired. The DoD IT Standards Registry can be found at https://jasm.apps.mil.

(4) Internet Protocol Version 6.

All acquisitions of WLAN devices, systems, and technologies must be Internet Protocol version 6 capable in accordance with DoDI 8440.02.

3.2. UNCLASSIFIED WLAN SECURITY, CERTIFICATION, AND VALIDATION.

DoD Component heads must use unclassified WLAN products that are certified and validated for secure end-to-end communications. In accordance with DoDI 8510.01, DoD Component heads 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 devices, 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 as part of the NIST Cryptographic Module Validation Program (CMVP) in accordance with the Federal Information Processing Standards (FIPS) Publication 140. Existing FIPS 140 cryptographic modules that have not been revoked or moved to the historical list are considered valid (e.g., FIPS 140-2, FIPS 140-3). There are multiple valid 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.

Unclassified WLAN-enabled PEDs 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 may implement encryption either in software via the WLAN supplicant or in hardware via the WLAN network interface card.

(a) Software Based Encryption.

1. WLAN client supplicants supporting this configuration must disable, or otherwise preempt, the encryption capabilities of the WLAN client's network interface card so the encryption can be performed solely by the supplicant software.

2. WLAN client supplicants must implement AES GCMP for encryption as defined in IEEE Standard 802.11.

3. The AES GCMP encryption must be an approved and validated approach under the NIST CMVP as meeting FIPS 140.

(b) Hardware Based Encryption.

1. WLAN client NICs supporting this configuration must implement AES GCMP as defined in IEEE Standard 802.11 within network interface card hardware.

2. The AES GCMP encryption must be an approved and validated approach 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.

(a) WLAN infrastructure systems may be composed of either standalone (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").

(b) All WLAN infrastructure devices must implement AES GCMP as defined in IEEE Standard 802.11.

(c) The AES GCMP encryption must be an approved and validated approach 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 for the data to be deciphered.

(a) Credentials for authenticating to data at rest protection must be DoD-approved PKI credentials in accordance with DoDI 8520.02 and, where applicable, the December 20, 2019 DoD CIO Memorandum. For devices that cannot interface with or support PKI credentials, alternate authenticators may be used in accordance with DoDI 8520.03.

(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, onboard memory cards, memory expansion cards).

(c) 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.

1. Authentication must be implemented by WLAN client supplicants that comply with IETF EAP TLS standards for WLANs RFC 5216.

2. The approved algorithms (e.g., hash message authentication code, secure hash standard) implemented during the EAP authentication process must be an approved and validated approach under the NIST CMVP as meeting FIPS 140.

(b) Authentication Server.

1. Authentication servers are responsible for authenticating user or device credentials during EAP TLS authentication, some also transmit the keying information that enables the AES GCMP 4-way handshake as defined in IEEE Standard 802.11.

2. 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.

3. The authentication server must transmit the keying information to the AP via a separate process.

a. EAP Authentication. DoD Component heads 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.

b. Encrypted Key Wrapping. DoD Component heads 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.

b. National Information Assurance Partnership (NIAP) Validation.

Any cybersecurity 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 PP (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 devices, systems, and technologies must be NIAP CC validated.

(a) WLAN devices and infrastructure must be validated under the NIAP CC as meeting applicable USG-approved WLAN access systems or client systems PP.

(b) WLAN access system is a PP module, so it must be part of a larger evaluation that is based on a base PP (e.g., network device collaborative PP).

(c) WLAN client is a PP module and must be part of a larger evaluation based on a base PP (e.g., mobile device fundamentals, general purpose operating system).

(d) When a logical boundary is employed, WLAN controllers with integrated firewalls must be validated as meeting the USG-approved firewall PP.

(2) Authentication Server.

Authentication servers must be validated under the NIAP CC as meeting the USG-approved authentication server PP.

(3) Cybersecurity Products.

WLAN-enabled PEDs must meet DoD cybersecurity requirements in accordance with DoDI 8500.01.

(a) DoD Component heads can employ cybersecurity products (e.g., firewalls, file integrity checkers, virus scanners, intrusion detection systems, anti-malware software) to meet DoD cybersecurity requirements.

(b) Cybersecurity products must be validated as meeting applicable USG-approved PP under the NIAP.

(4) WIDS/WIPS.

DoD Component heads must use WIDS as either integrated or standalone on all WLANs to passively detect and alert administrators to unauthorized WLAN activity for DoD WLANs, in accordance with DoDD 8100.02.

(a) DoD Component heads may use WIPS to stop suspicious activity on DoD WLANs following a determination by the AO.

(b) WIDS/WIPS must be validated under the NIAP CC as meeting the USG-approved WIDS/WIPS PP.

(5) VPN.

(a) WLAN-enabled PEDs must use a VPN with Internet Protocol Security (IPsec) or TLS to remotely connect over non-DoD WLAN networks in accordance with the DISA VPN Security Requirements Guide (SRG).

(b) VPNs must be validated as meeting applicable USG-approved PP under the NIAP.

c. Validated Physical Security.

(1) APs used in unclassified WLANs should not be installed in unprotected environments due to an increased risk of tampering or theft.

(2) If installed in unprotected environments, APs that store plaintext cryptographic keying information must be protected with added physical security to mitigate risks.

(a) DoD Component heads may choose products that meet FIPS 140 overall level 2, or higher, validation to verify that the AP provides validated tamper evidence, at a minimum; or

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

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 Component heads must use standards-based EAP TLS authentication to authenticate unclassified WLAN users or devices. Unclassified WLAN-enabled PEDs 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) DoD-approved PKI is the primary method of authentication to DoD information, systems, and devices in accordance with DoDI 8520.02 and DoDI 8520.03. For alternate methods of authentication and situations when these alternate methods of authentication are permitted see DoDI 8520.03.

(2) Unclassified WLAN-enabled PEDs may employ DoD Mobile PKI credentials in accordance with DoDI 8520.02 and the December 20, 2019 DoD CIO Memorandum.

(a) Non-DoD WLAN-enabled PEDs must comply with the requirements in the August 10, 2022 DoD CIO Memorandum.

(b) Authentication at the device and network levels may be achieved by assessing the combined processes of WLAN authentication and domain authentication.

c. DoD Component heads 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 GCMP 4-way handshake key exchange as defined in IEEE Standard 802.11.

(3) WLAN devices and infrastructure must be WPA3 Enterprise 192-bit mode or later version WFA certified to confirm authentication can be negotiated in a mixed vendor WLAN system implementation.

(4) Where WPA3 Enterprise 192-bit mode or later version 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 TLS 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.

3.4. NON-DOD UNCLASSIFIED WLAN SYSTEMS.

DoD Component heads must require DoD users of DoD WLAN-enabled PEDs on unclassified external WLAN systems, that are not DoD owned or operated, to employ standards compliant with Paragraph 3.4.b. and controls validated in accordance with Paragraph 3.4.c.

a. Non-DoD owned or operated include WLANs that are:

(1) Provided by commercial entities such as public or open hotspots;

(2) Home Wi-Fi;

(3) Not-for-profit entities;

(4) Federal partners; or

(5) Research, development, and test and evaluation environments.

b. DoD users of non-DoD WLAN systems must employ WPA3 Personal or later version, where WPA3 Enterprise 192-bit mode or later version is not available, or Passpoint (IEEE 802.11u) with AES encryption certified by the WFA for device security communications interoperability.

c. Security Certification and Validation.

(1) DoD users of non-DoD WLAN systems must immediately establish a connection to the DoD network via an approved method (e.g., IPSec VPN or TLS VPN) before login, in accordance with the DISA Virtual Private Network SRG.

(2) DoD users of non-DoD WLAN systems must employ controls to safeguard DoD information in accordance with their respective Component's policies and procedures consistent with DoDI 1035.01, DoDI 8500.01, and DoDI 8582.01. If DoD users cannot employ controls, they must not use the external WLAN system.

(3) Unclassified DoD WLAN-enabled PEDs must be protected in accordance with their respective Component's policies and procedures.

3.5. GUEST ACCESS FOR UNCLASSIFIED WLAN SYSTEMS.

a. DoD Component heads must require DoD owned and operated unclassified WLANs provide guest access to internet connectivity for DoD users with a DoD WLAN-enabled PED in accordance with the August 10, 2022 DoD CIO Memorandum and the DISA Network Infrastructure Policy STIG. DoD Component heads may require DoD owned and operated unclassified WLANs provide access to enterprise resources, for DoD users with a DoD WLAN-enabled PED.

b. Unclassified WLAN systems may provide guest access to internet connectivity for DoD users and non-DoD users with a non-DoD WLAN-enabled PED in accordance with the applicable DISA STIGs.

c. Guest user internet connectivity traffic must be segmented by a boundary with additional controls (e.g., spectrum sweeps).

(1) This segmentation is important to isolate guest user traffic and can be accomplished by logical separation (e.g., guest user open systems interconnect layer 3 access originating in an internet demilitarized zone outside of the enterprise network) or physical separation (e.g., an additional network only for guest user internet connectivity).

(2) The AO must determine which separation is appropriate based on a risk assessment and whether guest users must be sponsored by host organizations to include associated user agreements.

d. Unclassified WLAN systems are prohibited from sharing infrastructure with classified networks regardless of tunneling or logical segmentation. Unclassified WLANs with guest user 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 Component heads may operate unclassified WLAN systems and DoD WLAN-enabled PEDs in accredited collateral classified spaces (i.e., non-SCI and non-SAP) when authorized with written approval from the cognizant security authority in consultation with the AO(s) (for the unclassified system and PEDs, and the classified system(s) in the space), a review by the CTTA, and must comply with:

a. Joint approval from the USD(I&S) and the DoD CIO is required to operate unclassified and classified WLAN systems in the same space.

b. Unclassified WLAN-enabled PEDs in collateral classified spaces must have internal (built in) webcams and microphones physically disabled in accordance with the June 4, 2021 OSD Memorandum. Unclassified WLAN-enabled PEDs in collateral classified spaces in the Pentagon must also comply with the May 22, 2018 Deputy Secretary of Defense memorandum.

c. Industry standards, security certification and validation, and authentication of Paragraphs 3.1., 3.2., and 3.3. of this issuance.

d. Operate in accordance with:

(a) CNSS Directive No. 510.

(b) CNSS Policy No. 300.

(c) DoDD 8100.02.

(d) The Network Infrastructure Policy STIG.

(e) Paragraph 3.10 of this issuance.

e. Meet technical surveillance countermeasure requirements.

3.7. UNCLASSIFIED WLAN IN NEW FACILITIES.

a. DoD Component heads must include unclassified WLAN systems and associated security measures in new unclassified DoD facilities, where NIPRNET access is required, during the planning stage and, as determined by threat assessment, in accordance with the Unified Facilities Criteria 1-200-01 and the May 29, 2002 Under Secretary of Defense, Acquisition, Technology and Logistics Memorandum, which provides:

(1) Protective design planning.

(2) Construction.

(3) Sustainment.

(4) Restoration.

(5) Modernization criteria for facilities.

b. New WLAN systems may require infrastructure improvements (e.g., power, cabling, distributed antenna systems).

3.8. CLASSIFIED WLAN SECURITY, CERTIFICATION, AND VALIDATION.

DoD Component heads must require that classified WLAN systems are appropriately categorized and authorized by an AO in accordance with DoDI 8510.01. DoD Component heads must require that management of the implementation and use of classified DoD WLAN-enabled PEDs is performed in accordance with the guidance in the September 25, 2015 OSD Memorandum. Classified DoD WLAN-enabled PEDs connecting to the Commercial Solutions for Classified (CSfC) registered WLAN must be CSfC certified or a component of a CSfC solution. The use of classified WLAN-enabled PEDs in classified spaces in the Pentagon must be approved, jointly, by the USD(I&S) and DoD CIO, in accordance with the May 22, 2018 Deputy Secretary of Defense memorandum.

a. Cryptographic Protection of Classified WLAN Systems.

All National Security Systems (NSSs) to include classified WLAN systems must use NSA-certified or approved cryptography in accordance with all applicable policies governing NSSs. NSA's processes for these include:

(1) CSfC solutions, in accordance with Deputy National Manager for NSS approved CSfC capability packages (CP).

(a) These solutions must be registered with NSA's CSfC Program Management Office against one of the current applicable CPs in accordance with CNSS Policy No. 7.

(b) Solution components acquired for use in these solutions are validated for security functional requirements in accordance with CNSS Policy No. 11.

(c) The applicable CPs include:

1. Campus Wireless Local Area Network CP – encryption layers include WPA3 Enterprise 192-bit mode or later version and IPsec.

2. Mobile Access (MA) CP – encryption layers include IPsec and IPsec or TLS. In the case where a WLAN system is required to support a MA CP solution deployment, a USG private Wi-Fi (or Wireless) Networks, as defined in the MA CP must be accredited as an

unclassified WLAN specifically accredited to transport classified data that has been encrypted in accordance with the MA CP requirements.

(2) Government off the shelf, certified cryptographic products in accordance with their prescribed use and doctrine.

(3) Special purpose solutions approved by the Deputy National Manager for NSS.

b. Physical Security of Classified WLANs.

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

(2) Physical or electronic inventories may be completed 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 to limit signal propagation. See Director National Intelligence Executive Correspondence ES 2017-00043 for requirements in SCIFs.

(4) DoD mobility classified capability SECRET and TOP SECRET users must maintain continuous physical control of the hotspot (i.e., WLAN AP) or store in a locked container, following the requirements and specifications established by the AO, in accordance with the appropriate DoD mobility classified capability user agreement.

c. Cybersecurity for Classified WLANs.

Implementation of classified WLAN devices, systems, and technologies must:

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

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

(3) Employ authentication measures for the WLAN devices, systems, and technologies, in accordance with CNSS Policy No. 22 and National Security Memorandum 8. Classified DoD WLAN-enabled PEDs used to access DoD NSS PKI enabled enterprise services (e.g., SIPRNET e-mail) must support DoD NSS 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 DISA Connection Approval Office. Written operating procedure or policy must describe procedures for the protection, handling, accounting, and use of NSA-approved cryptographic solutions.

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

(7) Be permitted in a U.S. permanent SCIF, or temporary SCIF (T-SCIF), or secure working area, or temporary secure working area, if approved, in accordance with Director, National Intelligence Executive Correspondence ES 2017-00043, IC Directive Number 705, IC Directive Number 503, and DIA SCIF policy requirements.

(8) Require a CTTA review before installation and operation of WLANs intended for use in processing or transmitting classified information, in accordance with CNSS Policy No. 300.

(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-approved encryption at a level consistent with the classification of the data stored on the device in accordance with the CSfC Campus WLAN CP, MA CP, 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;

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

(4) Retained in an approved open storage facility.

3.9. WLAN INTRUSION DETECTION AND PREVENTION.

DoD Component heads must implement a WIDS that allows for continuous monitoring of WLAN activity and the detection of WLAN related policy violations on all unclassified and classified DoD WLANs.

a. DoD Component heads may implement WIPS to stop suspicious activity on unclassified and classified DoD WLANs.

b. DoD Component heads must complete an assessment of the DoD WLANs local environment to identify potential vulnerabilities and evaluate risk before the AO decides to employ or not to employ a WIPS.

c. WIDS and WIPS implementation must be in accordance with:

(1) The CSfC Campus WLAN CP.

(2) CSfC WIDS/WIPS Annex.

(3) CSfC Continuous Monitoring Annex.

(4) Intrusion Detection and Prevention System SRG.

(5) Network Infrastructure Policy STIG.

(6) CNSS Policy No. 17.

(7) Paragraph 3.10 of this issuance.

d. DoD Component heads must verify that WIPS does not impact the performance of WIDS (e.g., utilization factor).

e. DoD Component heads must consult with legal counsel and the SCOP to develop a common understanding of the legal (i.e., civil liberties) and privacy considerations related to the use of WIPS and the collection of data before implementation.

(1) WIDS/WIPS Monitoring Requirements.

The WIDS and WIPS (if employed) must be capable of monitoring IEEE 802.11 transmissions within all DoD WLAN environments and detect nearby unauthorized WLAN devices. WIDS/WIPS are not required to monitor non-IEEE 802.11 transmissions.

(2) WIDS/WIPS Implementation Criteria.

The WIDS and WIPS (if employed) must continuously monitor (i.e., scan for and detect) authorized and unauthorized WLAN activities 24 hours a day, 7 days a week within a DoD WLAN environment.

(a) Scanning must include a location sensing capability that enables designated personnel to geo-locate to within a specified distance as determined by the AO; identify the activity; and take appropriate actions, which includes technical and counterintelligence measures, and notification of security and/or law enforcement to mitigate IEEE 802.11 threats.

(b) The WIDS/WIPS must be integrated with DoD Component security or law enforcement, technical surveillance countermeasures, network management systems, including sharing full location data, and be configured for effective event handling in accordance with DoDI 8410.03.

(c) DoD Component heads must develop and execute incident response plans for WIDS/WIPS events to include technical surveillance countermeasures, counterintelligence, and security or law enforcement roles and responsibilities.

3.10. DOD SRG AND STIG COMPLIANCE.

DoD Component heads must incorporate the security best practices specified in the Network Infrastructure Policy STIG, Network WLAN STIG, along with other applicable SRGs and STIGs as they pertain to the implementation of WLANs.

a. DoD Component heads must comply with applicable NIAP PP.

b. If NIAP PP are not published, compliance with SRGs is acceptable.

3.11. WLAN SPECTRUM SUPPORTABILITY.

a. Component heads must:

(1) Require spectrum supportability before acquiring spectrum dependent WLAN systems in accordance with DoDD 3610.01 and DoDI 4650.01.

(2) Require compliance with the DoD Electromagnetic Environmental Effects Program in accordance with DoDI 3222.03.

(3) Require adherence with military standards (MIL-STDs) that are applicable to the installation and operation of WLANs, in accordance with MIL-STD 461G and MIL-STD 464D.

b. DoD requires non-licensed devices operating in the United States and its possessions to be registered with the local spectrum management office for IEEE 802.11 series.

(1) Outside the United States and its possessions, each theater commander must determine, with support of the spectrum management process, if frequency support is available and authorized, considering any potentially applicable agreements with host nations.

(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.

c. DoD standard frequency assignment format request for WLAN applications will contain an entry noting "this circuit must comply with the latest DoDI 8420.01 enterprise encryption requirements." Line 520 of a standard frequency assignment format should be used for this entry so authorized users comply with latest encryption requirements, such as current WPA3-Enterprise 192-bit mode encryption requirements or later version for WLAN.

3.12. INDUSTRY STANDARD WAVEFORM MODIFICATIONS.

a. To verify 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.

b. 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.

DoD Component AOs are authorized to grant exceptions to the use of unclassified WLAN devices, systems, or technologies with written notification to DoD CIO to inform WLAN lessons learned and future requirements.

(1) Non-Compliant WLAN Devices, Systems, or Technology Exceptions.

(a) 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.

1. 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).

2. AOs must review the risk management framework authorization package to make an informed decision about the impact to interoperability before granting an exception.

(b) Exceptions for the Use of NSA-certified Devices on Unclassified WLANs.

1. Use of NSA-certified products are also acceptable for unclassified data, when operating in the secure mode.

2. 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.

(c) Exceptions for Minimal Impact WLAN Systems.

1. Exceptions may be granted by the AO for minimal impact WLAN systems.

2. These systems must be segmented from the DoDIN via a wireless demilitarized zone that is WIDS/WIPS capable, as described in Paragraph 3.9., and limits ports and protocols to the minimum set necessary to achieve mission objectives.

3. A STIG compliant firewall must be located at the system's point of entry onto the DoDIN.

(2) Unclassified WLAN Backhaul Exceptions.

(a) 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.

(b) DoD Component AOs 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 WLAN operating environments.

(a) This exception allows the AO to implement periodic scanning conducted by designated personnel using handheld scanners during walkthrough assessments.

(b) 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 WLAN Security 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.

ACRONYM	MEANING
AES	advanced encryption standard
AMD	approved mobile device
AO	authorizing official
AP	access point
CC	common criteria
CIO	chief information officer
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
DIRNSA/CHCSS	Director, National Security Agency / Chief, Central Security Service
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDIN	Department of Defense Information Network
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standards
G (telecommunication standard)	generation
GCMP	Galois or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
IA	information assurance
IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPsec	Internet Protocol security
IT	information technology
ISO	International Organization for Standardization

ACRONYM	MEANING
JITC	Joint Interoperability Test Command
MA	mobile access
MAC	medium access control
MIL-STD	military standard
NIAP	National Information Assurance Partnership
NIPRNET	Nonclassified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
PED	portable electronic device
PKI	public key infrastructure
PP	protection profiles
RF	radio frequency
RFC	request for comment
SAP	special access program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SCOP	Senior Component Official for Privacy
SIPRNET	SECRET Internet Protocol Router Network
SRG	security requirements guide
STIG	security technical implementation guide
TLS	transport layer security
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	U.S. Government
VPN	virtual private network
WFA	Wireless Fidelity (Wi-Fi) Alliance
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
WPA3	Wi-Fi Protected Access 3

G.2. DEFINITIONS.

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

TERM	DEFINITION
AES GCMP	An encryption algorithm that utilizes 128-bit block ciphers to provide authentication and privacy.
AMD	Defined in the August 10, 2022 DoD CIO Memorandum.
authentication	A method used to secure computer systems or networks by verifying a user's identity, requiring two factors to authenticate (i.e., 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 (IETF RFC 5080) as an authentication server, which is part of a WLAN system. Authentication servers interconnect with WLAN infrastructure over the distribution (also called 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 GCMP 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 can internally generate the keying information, thereby not requiring the transmission of keying information from authentication servers.
cellular technology generations (G)	2.5G, 3G, 4G or long-term evolution, 5G cellular systems, etc.

TERM	DEFINITION
CTTA	An experienced, technically qualified USG employee who has met established certification requirements in accordance with CNSS approved criteria and has been appointed by a USG department or agency to fulfill CTTA responsibilities.
cybersecurity	Replaced IA, defined in CNSS Instruction No. 4009.
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 or interrogator.
DoD user	Authorized DoD employees (government and contractor).
DoD WLAN-enabled PED	DoD owned and operated IEEE 802.11 capable WLAN-enabled PED that transmits, receives, processes, or stores unclassified and classified information, includes AMDs.
geo-locate	The process of determining the physical location of a WLAN-enabled PED, either via GPS, cellular network, Wi-Fi system, Bluetooth signal, or IP address tracking.
guest access	WLAN access provided to a non-organizational user.
IA	Replaced by the term "cybersecurity" as defined in DoDI 8500.01 and CNSS Instruction No. 4009.
IEEE 802.1X	An IEEE standard that performs network access control by utilizing EAP to provide authentication to WLAN devices.
IEEE 802.11	An IEEE body of standards that operate in the 2.4, 3.6, 4.9/5, 6, and 60 gigahertz spectrum bands to provide communication in WLAN environments. The family of standards is comprised of the IEEE Standard 802.11-2020 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. Versions of the 802.11 family of standards are also identified as Wi-Fi. For example, 802.11ac is called Wi-Fi 5, 802.11ax is Wi-Fi 6/6E, and 802.11be is Wi-Fi 7, with future generations' names to be determined.

TERM	DEFINITION
IEEE 802.15	A body of standards for "Wireless Personal Area Networks" (WPANs) which means short-range wireless communication between portable devices like smartphones, computers, and other nearby electronics within a personal operating space, commonly associated with technologies like Bluetooth; encompassing both the physical layer and MAC aspects of such networks.
IEEE 802.16	A body of standards established by the IEEE to enable 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 WLAN 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-TLS 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 confirms the most efficient technology is utilized 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.

TERM	DEFINITION
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. 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.

TERM	DEFINITION
physically disabled	A method of disablement that cannot be made or reversed, by privileged or non-privileged users or administrators, through logical settings configured by software (such as applications, operating systems, firmware, basic input/output system (known as "BIOS"), or unified extensible firmware interface UEFI), or otherwise configured in volatile or non-volatile memory or storage.
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 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 disassociate 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 enough 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, 6, and 60 gigahertz) and transceivers that are like IEEE 802.11 but operate in non-standard frequency band.

TERM	DEFINITION
WLAN	A group of wireless APs and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired local area networks to provide enhanced user mobility.
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, PDA, 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.
WPA3	An encryption standard introduced by the Wi-Fi Alliance in 2018 to replace the 2004 WPA2 and mandatory as of July 2020 for all new Wi-Fi CERTIFIED™ devices. Simplifies Wi-Fi security, including enabling better authentication, increased cryptographic strength, and requiring the use of Protected Management Frames to increase network security. WPA3 has two modes – Personal and Enterprise with the former for DoD PEDs that cannot access a DoD owned and operated WLAN and the latter for accessing DoD owned and operated WLANs. WPA3-Enterprise mode using 192-bit, with Commercial National Security Algorithm in accordance with CNSS Policy No. 15 Annex B, replaced the less secure WPA2 pre-shared key as the DoD encryption standard for DoD WLAN systems.
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/01-13, "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. 15, "Use of Public Standards for Secure Information Sharing," October 20, 2016

Committee on National Security Systems Policy No. 17, "Policy on Wireless Systems," January 14, 2014

Committee on National Security Systems Policy No. 22, "Cybersecurity Risk Management," September 2021

Committee on National Security Systems Policy No. 300, "National Policy on Control of Compromising Emanations," April 2004

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Committee on National Security Systems Directive No. 510, "Directive on the Use of Mobile Devices Within Secure Spaces," November 20, 2017

Commercial Solutions for Classified Annex 1.1.0, "Continuous Monitoring," March 2, 2021

Commercial Solutions for Classified Annex V1.0, "Wireless Intrusion Detection System/Wireless Intrusion Prevention System (WIDS/WIPS)," February 2, 2021

Commercial Solutions for Classified Capability Package V3.0, "Campus Wireless Local Area Network," May 4, 2022

Commercial Solutions for Classified Capability Package V5.0, "Data at Rest," November 18, 2020

Commercial Solutions for Classified Capability Package 2.5.1, "Mobile Access," February 18, 2022

Defense Information Systems Agency Security Requirements Guide (SRG) Version 2 Release 6, "Intrusion Detection and Prevention System," July 24, 2020

Defense Information Systems Agency Security Requirements Guide (SRG), "Virtual Private Network (VPN)," May 4, 2023

Defense Information Systems Agency Security Technical Implementation Guide (STIG) Version 10 Release 6, "Network Infrastructure Policy," June 7, 2023

Defense Information Systems Agency Security Technical Implementation Guide (STIG), "Network WLAN," April 27, 2023

Director National Intelligence Executive Correspondence ES 2017-00043, "Wireless Technology in the Intelligence Community," January 19, 2017

DoD Chief Information Officer Memorandum, "Use of Non-Government Owned Mobile Devices," August 10, 2022

DoD Chief Information Officer Memorandum, "DoD Mobile Public Key Infrastructure (PKI) Credentials," December 20, 2019

DoD Chief Information Officer Memorandum, "Department of Defense Transition to Stronger Public Key Infrastructure Algorithms," December 23, 2022

DoD Directive 3610.01, "Electromagnetic Spectrum Enterprise Policy," September 4, 2020

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020, as amended

DoD Directive 5105.21, "Defense Intelligence Agency," January 25, 2023

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

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

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, 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," October 5, 2020

DoD Instruction 1035.01, "Telework And Remote Work," January 8, 2024

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

DoD Instruction 4630.09, "Communications Waveform Management and Standardization," November 23, 2020

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 Adaptive Acquisition Framework," January 23, 2020, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM)," April 3, 2014, as amended

DoD Instruction 8310.01, "Information Technology Standards in the DoD," April 7, 2023

DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022

DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012, as amended

DoD Instruction 8440.02, "DoD Implementation of Internet Protocol Version 6," December 17, 2024

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8520.02, "Public Key Infrastructure and Public Key Enabling," May 18, 2023

DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 19, 2023

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

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

Executive Order 12333, "United States Intelligence Activities," December 4, 1981

Executive Order 13526, "Classified National Security Information," December 29, 2009

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

Federal Information Processing Standards Publication 140-3, "Security Requirements for Cryptographic Modules," March 22, 2019

Institute of Electrical and Electronics Engineers Standard 802.11-2020, "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," February 26, 2021[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: 2022, "International Standard - Telecommunications and Information Exchange Between Systems - Specific Requirements for Local and Metropolitan Area Networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," October 26, 2022[2]

Internet Engineering Task Force Request for Comment 4017, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs," March 2005[3]

Internet Engineering Task Force Request for Comment 5080, "Common Remote Authentication Dial In User Service Implementation Issues and Suggested Fixes," December 2007[3]

Internet Engineering Task Force Request for Comment 5216, "The EAP-TLS Authentication Protocol," March 2008[3]

Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017[4]

Military Standard-461G, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," December 11, 2015

[1] Copies may be obtained at https://ieeexplore.ieee.org/document/9502043
[2] Copies may be obtained at http://ieeexplore.ieee.org/document/9930960
[3] Copies may be obtained at https://www.ietf.org
[4] Copies may be obtained at https://media.defense.gov

Military Standard-464D, "Electromagnetic Environmental Effects Requirements for Systems," December 24, 2020

National Information Assurance Partnership Protection Profile V3.2, "Mobile Device Fundamentals," April 15, 2021

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

National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022

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

Office of the Secretary of Defense Memorandum, "Collaboration Peripherals in Secure Spaces," June 4, 2021

Office of the Deputy Secretary of Defense Memorandum, "Mobile Device Restrictions in the Pentagon," May 22, 2018

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

Unified Facilities Criteria 1-200-01, "DoD Building Code." September 1, 2022, as amended

[5] 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