Department of the Army
Pamphlet 25–2–9

Information Management: Army Cybersecurity

Wireless Security Standards

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–9
Wireless Security Standards

This new Department of the Army pamphlet, dated 8 April 2019—

- Provides guidance for the vetting, approval, acquisition, and use of wireless technology and wireless-enabled tools within the Department of the Army (throughout).

- Contains amplifying procedures and guidance to DODI 8100.04 and the Army use of the Department of Defense Unified Capabilities Approved Products List (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–9

Information Management : Army Cybersecurity

Wireless Security Standards

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This is a new Department of the Army pamphlet.

Summary. This pamphlet provides guidance for the vetting, approval, acquisition and use of wireless technologies within the Department of the Army. It supports AR 25–2 and the Army Cybersecurity program. This pamphlet provides amplifying procedures and guidance to DODI 8100.04.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent for this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (cio-6.policy.inbox@mail.mil).

Distribution. This regulation is available electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

UNCLASSIFIED

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
This pamphlet provides guidance for the vetting, approval, acquisition, and use of wireless technology within the Department or the Army (DA), and leverages applicable Department of Defense (DOD) and DA publications. It amplifies procedures and provides guidance to DODI 8100.04 and the Army use of the DOD Unified Capabilities (UC) Approved Products List (APL). This pamphlet also addresses the process for acquiring wireless technology tools on the DOD UC APL, and explains the roles and duties within the DOD UC APL process. The DOD UC APL process provides for an increased level of confidence through cybersecurity and interoperability certification.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Applicability
This publication applies to all Army-owned, controlled, or contracted wireless networks, systems, and devices that process, store, or transmit unclassified information. This pamphlet does not apply to the vetting processes of open source technologies, cross domain solutions, protected distributed systems, and communications security technologies requiring National Security Agency (NSA)-approved key management (such as suite A and suite B).

1–5. Department of Defense Unified Capabilities Approved Products List process
a. The DOD UC APL was established in accordance with the DOD Unified Capabilities Requirements (UCR). The DOD UC APL process was developed in accordance with DODI 8100.04 and is managed by the Defense Information Systems Agency (DISA) Network Services Unified Capabilities Certification Office. Use of the DOD UC APL allows DOD components to purchase and operate UC systems over all DOD network infrastructures (see DODI 8100.04).

b. According to AR 25–2, the Army will use the DOD UC APL when purchasing all cybersecurity or cybersecurity-enabled hardware, firmware, and software components (excluding cryptographic modules).

Chapter 2
Wireless security standards

2–1. Administrative requirements
a. Authorizing official. The authorizing official (AO), appointed in accordance with AR 25–2, is responsible for ensuring that all wireless local area network (WLAN) and portable electronic device (PED) technologies (for example, smartphones, tablets) adhere – at a minimum – to the requirements outlined in AR 25–2 and this DA PAM. For non-compliant wireless implementations, the AO is responsible for approving and maintaining mitigation plans as part of their acceptable level of risk determination.

b. Network enterprise centers. Network enterprise centers (NECs) and local area networks (LANs) consist of all network enclaves below the Top Level Architecture stack, to include all tenant installations. NECs will identify and monitor all wireless gateways and access points (APs) on their enclave network. No wireless devices or networks will operate on the NEC's infrastructure unless they have been approved by the AO for the installation's networks, and the systems are authorized.

c. Authorization to operate/authorization to connect. All wireless networks and devices must be assessed and authorized prior to being approved to operate on the NEC's LAN. All unauthorized wireless devices and networks will be rendered inoperable and restricted from use until an approval is granted through the Army's Risk Management Framework (RMF) process.

d. Mitigation plan. Fielded wireless LAN and PED technologies that are not in compliance with this DA PAM must have mitigation plans developed and submitted to the designated system AO within 90 days, which establishes the systems milestone to meet the requirements of this DA PAM.

e. Assessments. The Information System Security Manager will ensure wireless assessment scans are performed on a monthly basis on their respective Information Systems (ISs) via the DOD-approved Wireless Discovery Device and mapping tool. Maintain scanning reports and logs for a minimum of 1 year. See paragraph 2–2*d*.

2–2. Wireless local area network requirements

a. Configure wireless solutions to prevent or preclude backdoors into the Army's LANs. Backdoors, poor access management, and misconfigurations can be caused by unprotected transmissions or unprotected PEDs connecting to a network. Systems must also meet all applicable Information Assurance Vulnerability Message compliance requirements.

b. Where wireless LANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information interception/monitoring and network intrusion prior to installation of these devices. Only properly trained cybersecurity personnel can successfully determine these risk factors. Cybersecurity personnel accomplishing these tasks must meet all training/certification requirements outlined in DOD Directive (DODD) 8140.01.

c. Fielded wireless LANs and PEDs with connectivity to the Department of Defense Information Network must meet the RMF security requirements outlined in DODI 8510.01.

d. All wired and wireless networks require the use of Wireless Intrusion Detection Systems (WIDS), capable of location detection of both authorized and unauthorized wireless devices. All systems will provide 24/7 continuous scanning and monitoring (see para 2–1*e*). Appointed NEC personnel will respond to all WIDS alerts, maintain reports, and document actions taken. Maintain WIDS logs and documented actions for a minimum of 1 year. For incidents, the appointed NEC personnel will review the incoming event data, identify what type of activity is occurring, and determine if an anomalous event shall be treated as a reportable cyber event or incident. For further guidance on incident handling refer to Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B.

2–3. Component configuration requirements

a. Commercial-off-the-shelf products typically have factory default settings designed for ease of use that do not meet Army security requirements. Configure wireless equipment to meet current DOD and Army standards.

b. Wireless access points/access points (APs) use an Extended Service Set Identifier (ESSID) or Service Set Identifier (SSID) in determining the authorized group of mobile radios. Turn off the ESSID/SSID broadcast option at the AP.

c. The Institute of Electrical and Electronics Engineers (IEEE) 802.1X (Port Based Network Access Control) standard provides a framework for access control that leverages Extensible Authentication Protocol to provide centralized, mutual authentication. The IEEE 802.1X framework provides the means to block user access until authentication is successful, thereby controlling access to WLAN resources.

2–4. Authentication

All WLAN solutions must provide for strong (two-factor) authentication at the network and device level. WLAN solutions must be IEEE 802.11i (Wi-Fi Protected Access II) compliant and Wi-Fi Protected Access 2 (WPA2) Enterprise Certified. IEEE 802.11i and WPA2 implement IEEE 802.1x access controls with Extensible Authentication Protocol – Transport Layer Security mutual authentication in a configuration that ensures the exclusive use of Federal Information Processing Standard (FIPS) 140–2 validated Advanced Encryption Standard – Counter Mode with Cipher Block Chaining – Message Authentication Code Protocol communications.

2–5. Protection of national security information

Any wireless solution that transmits data of a National Security nature (that is, National Security Information [NSI], Secret and below information) must protect data-in-transit with NSA-approved Suite B encryption in accordance with Committee on National Security Systems Policy (CNSSP) 15, CNSSP 17, DODD 8100.02 (Use of Commercial Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)), and Public Law (PL) 107–347.

2–6. Encryption

a. All wireless implementations must provide for end-to-end encryption of data-in-transit through the use of validated and approved National Institute of Standards and Technology (NIST)/NSA cryptographic schemes, as dictated by data classification. Wireless devices will meet the requirements FIPS 140–2 Level 2 compliancy as the end-state requirements for cryptography.

b. At a minimum, the security controls in wireless solutions will have a Common Criteria evaluation rating of Evaluation Assurance Level (EAL) 2 based upon the current National Information Assurance Partnership (NIAP) protection profile. EAL 4 will be the end state when a NIAP protection profile is available at that level.

c. NSA-approved Type 1 or Suite B encryption must be used for any situation requiring protection of any classified information.

d. Tactical environments must use NSA-approved cryptography. Only under special circumstances will wireless (802.11) with NIST-approved FIPS 140–2 Level 2 validated cryptographic modules be granted an exception for use in a tactical environment. These exceptions will be approved on a case-by-case basis by Headquarters, Department of the Army, CIO/G–6.

2–7. Bridging, multi-point, and point-to-point technologies and topologies

a. The IEEE 802.11 series is the industry standard for WLAN equipment, and is the standard to consider when acquiring WLANs. If bridges are used, they must utilize end-to-end encryption using FIPS 140–2 Level 2 validated cryptographic modules. There will be no exceptions granted when bridges connect into an Army backbone. Wireless ethernet bridges can generally be categorized by environment (indoor/outdoor), topology (point-to-point, multipoint), and type of technology (802.11b/g, 802.11a, 802.11n, 802.11ac, 802.11ad).

b. Wireless Metropolitan Area Network solutions, and "last mile" wireless point-to-point bridging solutions using technologies such as Worldwide Interoperability for Microwave Access (802.16), Millimeter Wave, and Free-Space Optics require Quality of Service protocols to ensure consistent service. Use Open System Interconnection (OSI) Layer 3 or OSI Layer 2 protection using FIPS 140–2 Level 2 encryption schemes with these bridging solutions. Implement Dual Layer protection using NSA-certified Type 1 or Suite B encryption to protect data on classified or mission critical (tactical) networks.

2–8. Wireless personal area networks

Wireless Personal Area Network (WPAN) communications (for example, Bluetooth, Zigbee, Ultra-Wideband (UWB) and similar technologies) require protection of data-in-transit using either NSA-approved or FIPS 140–2 validated encryption, as appropriate, unless the AO provides written approval to forgo the required NSA or FIPS mechanisms. Non-NSI WPAN solutions must use a FIPS 140–2 Level 2 validated encryption module as a minimum. Secure authentication between WPAN devices is required to operate with procured Army equipment or within an Army environment.

2–9. Remote access

Mobile users connecting to a commercial wireless service provider must follow the established U.S. Army Cyber Command-approved access procedures for identity access management to protect data-in-transit, data-at-rest, and the user's PED.

Chapter 3
Wireless devices

3–1. Wireless portable electronic device requirements

a. Wireless PEDs are considered extensions of a LAN environment, and must be configured in accordance with the appropriate DISA Secure Technical Implementation Guide (STIG) so that the security posture of the device and the Army network are not compromised. Some wireless PEDs can be equipped with Wi-Fi, Voice over Internet Protocol, and Global Positioning System functionality which could compromise Army networks.

b. Army commands and activities whose members use PEDs that synchronize with desktop or laptop computers on Army networks will adopt the following security measures and include them in the command IS Security Authorization Package (SAP), security policies, security awareness and training, and network user agreements:

(1) Only those applications approved by the AO will be approved for use.

(2) PEDs' wireless connectivity features (for example, Wi-Fi, Bluetooth) must not be enabled while the PED is connected to the Army network.

(3) Configure wireless PEDs in accordance with the appropriate DISA STIG and applicable System Administrator Standard Operating Procedures.

(4) Wireless PEDs must utilize an applicable enterprise server to both enhance security and improve remote management/policy enforcement capabilities.

(a) Security. PEDs with wireless communication capabilities are not permitted inside Sensitive Compartmented Information Facilities (SCIF), classified, or restricted areas without proper approval and the following minimum security modifications: the device's infrared (IR) port has been completely covered by metallic tape; and any wireless transmission capability (for example, antenna, radio module) has been removed or physically disabled. The agency in charge of any given SCIF, classified, or restricted area is the authority for the procedures to move PEDs in or out of their respective facilities, and will take all physical security steps necessary to prevent introduction of unauthorized devices inside a restricted space.

Note: Modifications of a PED in the manner described above may invalidate its warranty for the manufacturer.

(b) Authorization. Wireless devices such as laptops, PC tablets, and personal digital assistants connecting to a network will be included in the updated RMF process, and the RMF package will be signed by the AO. A thorough and comprehensive requirement validation, risk analysis, and an implementation and migration plan will be included within the required SAP. Wireless connectivity will not be authorized if the wired infrastructure that is to be extended is not authorized.

(c) Authentication. At no time will a PED without strong Identity and Access Management (IdAM) be used to store, process, or transmit official Army information. IdAM is the process of accepting a claimed identity and establishing the validity of that claimed identity. Strong IdAM is identified as two-factor authentication. PEDs without strong IdAM built in or added to the system will only be used for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.

(d) Encryption. Web-enabled PEDs that rely on Wireless Access Protocol (WAP) and/or use commercial wireless network providers are at risk for information compromise. Do not transmit data in this situation unless the data is encrypted end-to-end using a FIPS 140–2 validated cryptographic module. The WAP standard is evolving to support data confidentiality requirements through the use of Public Key Infrastructure digital certificates and by allowing customers to run their own WAP gateways for secure, direct connections to web-based resources.

(e) Data-at-rest. Unless the AO provides written approval to forgo this requirement, PEDs will fully comply with all mandated data-at-rest protection requirements.

(f) Anti-virus. To ensure a consistent level of protection against viruses and malware is implemented, it is important to maintain up-to-date signature files that are used to profile and identify viruses, worms, and malicious code. The network infrastructure must accommodate anti-virus software updates for all desktops and servers that support PEDs. PEDs must support anti-virus products and updating capabilities.

(g) Network scanning. Wireless PEDs that are connected to a network introduce risk when they are not fully secured, compliant with policy, and up-to-date on security patches. Therefore, connected wireless PEDs must be scanned in accordance with the same network scanning requirements for wired ISs and devices. (For example, vulnerability, compliance, and malware scans using tools such as Assured Compliance Assessment Solution. Further guidance and training on network scanning tools is available at (https://disa.deps.mil/ext/cop/mae/netops/acas/sitepages/home.aspx)).

3–2. Cordless phone

The use of cordless telephones to communicate sensitive information is prohibited unless the device can be properly encrypted with NSA-approved encryption. A cordless telephone is defined as a telephone unit that generally will only operate within a limited distance from its base station, usually 300 to 400 feet. In order to ensure that all personnel (active duty, Reservists, National Guard, civilians, and contractors) are aware of the telephone security requirements, organizations will include this policy in their local cybersecurity awareness training programs.

3–3. Wireless keyboards and mice

a. Wireless keyboards and mice that use Radio Frequency (RF) protocols (that is, WLAN technologies such as the 802.11-based standards and draft standards; WPAN 802.15-based standards such as Bluetooth, Coexistence, WiMedia, UWB, Zigbee; and any other RF protocol, whether standards-based or proprietary) are not authorized unless they use FIPS 140–2 validated cryptographic modules (if non-NSI data is processed) or NSA Suite B products (if NSI data is processed), and are approved for use by the AO in consultation with the Certified Tempest Technical Authority (CTTA).

b. Wireless keyboards and mice that use infrared (IR) are authorized for use on workstations/servers attached to the NIPRNet or SIPRNet, with the approval of the AO (in consultation with the CTTA). The area where the IR is to be used must be entirely enclosed with walls, ceiling, and floors consisting of material opaque to IR. Windows must have a film approved for blocking IR and doors must remain closed while devices are in operation.

c. There will be no mixing of classified and unclassified equipment using IR within the same enclosed area. In any enclosed space, IR can only be used on devices of the same security level. If IR is used with a classified device, all IR ports on unclassified devices in the space must be disabled using metallic tape. If IR is used with an unclassified device, all IR ports on classified devices in the space must be disabled using metallic tape and through use of device settings.

d. Any use of compliant IR wireless mice and keyboards in an area that electronically stores, processes, or transmits classified information must be approved by the AO in consultation with the CTTA.

e. Wireless keyboards may be vulnerable to interception of passwords, PIN numbers, and other sensitive information. Wireless mice and keyboards may also interfere with authorized wireless networks, wireless scanning, and WIDS.

3–4. Bluetooth

Commercial Bluetooth wireless headset solutions that do not meet DOD and Army Bluetooth security standards are prohibited by DOD and Army. Do not use Bluetooth devices to send, receive, store, or process classified information. CIO/G–6 Cybersecurity Directorate will continue to follow the progress of a secure Bluetooth devices based on specifications provided by NSA and DISA and approved by the DOD CIO.

3–5. Wearable fitness devices

Wearable fitness devices are authorized for introduction and use within Army offices, work spaces, and facilities authorized up to and including TOP SECRET collateral. This includes common areas, restricted areas, and collateral open storage areas, under the following circumstances. Authorized personal wearable fitness devices will receive only vendor-supplied software updates.

a. The device must be—

(1) Commercially available in the U.S. or at a U.S. Military Exchange.

(2) Marketed primarily as a fitness or sleep device.

(3) Capable of disabling wireless communication capabilities including any propriety synchronization capability which pairs the wearable fitness device with a mobile device or smartphone. Note: Bluetooth capabilities are exempt from this requirement.

(4) Designated as a Federal Communications Commission (FCC)-Class B digital device or FCC Class B exempt.

b. The device cannot contain the following capabilities or characteristics:

(1) Photographic or video capture/recording capabilities

(2) Microphone or audio recording capabilities.

c. The following restrictions apply to wearable fitness devices:

(1) Personnel will be cleared, at a minimum, to the same level of the facility in which the device will be introduced. (That is, if the facility is authorized at the secret level, the user will have at least a secret clearance).

(2) Accessories including the charging cables and/or any Universal Serial Bus accessories (for example, Bluetooth dongle) are not authorized within DOD spaces.

(3) The devices will not be connected to any government IS. This includes connections for charging and synchronization.

(4) Disable wireless and/or connectivity capabilities. If the device has wireless or connectivity capabilities which cannot be disabled, they are not authorized into the space. Bluetooth capabilities for wearable fitness devices are not required to be disabled.

d. Personnel bringing wearable fitness devices into DOD accredited spaces are consenting to inspection and monitoring of the devices. Wearable fitness devices in DOD accredited spaces are subject to inspection and, if necessary, technical evaluation. In addition, the emanations of authorized wearable fitness devices in DOD accredited spaces are subject to monitoring.

e. The local Cognizant Security Authority (CSA) may deem an accredited space exempt and continue to restrict wearable fitness devices if the following criteria applies:

(1) Any space that substantially or entirely involves the use of classified material acquired by another intelligence agency and that agency requests/supports the restriction.

(2) Any space accommodating another intelligence agency or foreign intelligence partner and that agency or partner requests/supports the restriction.

(3) Any space wherein the activity and/or discussion involves support to clandestine or covert operations. CSAs are responsible for updating all appropriate signage to reflect the authorization of wearable fitness devices within accredited DOD offices, workspaces, and facilities.

Chapter 4
Training

Portable electronic device

All users issued a PED must complete security awareness training regarding the physical and cybersecurity vulnerabilities of the device, prior to being granted network access through use of the device. This information will be included in the Acceptable Use Policy.

Chapter 5
Products

5–1. Wireless devices

a. All wireless devices including commercial unlicensed devices must be coordinated with the local Army frequency manager prior to purchase.

b. All wireless devices procured with Army funds must be certified for spectrum supportability through Military Command, Control, Communications, and Computers Executive Board, per DODD 5000.01 and AR 5–12. If a new solution is available, but not previously considered by the MC4EB, submit a spectrum supportability request DD–1494 to the Army Spectrum Management Office, 6916 Cooper Avenue, Fort Meade, MD 20755–7901.

5–2. Approved and procured products

a. Approved products are listed on the DOD UC APL (https://aplits.disa.mil), or specified as approved in current, signed CIO/G–6 issuances. Army customers who wish to have cybersecurity or cybersecurity-enabled products considered for the DOD UC APL must contact the Army CIO/G–6 Cybersecurity Directorate to coordinate sponsorship.

b. Procure products through the Army Computer Hardware Enterprise Software and Solutions (CHESS) program (https://chess.army.mil/content/page/res_contprog). Purchase products not available through CHESS using an existing DOD Enterprise License Agreement (ELA) or DOD Blanket Purchase Agreement (BPA), such as via the DOD Enterprise Software Initiative (ESI). Products listed on CHESS or DOD ELA / BPA / ESI are not to be considered pre-approved for any purpose. Army organizations must also refer to AR 25–1 and follow the process to obtain a Certificate of Networthiness, as required.

Appendix A

References

Section I

Required Publications

AR 5–12
Army Use of the Electromagnetic Spectrum (Cited in para 5–2*b*.)

AR 25–1
Information Technology (Cited in para 5–2*b*.)

AR 25–2
Army Cybersecurity (Cited in para 2–1*a*.)

CJCSM 6510.01B
Cyber Incident Handling Program (Cited in para 2–2*c*.) (Available at http://www.jcs.mil/library/cjcs-manuals/.)

CNSSP 15
Use of Public Standards for Secure Information Sharing (Cited in para 2–5.) (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

DODD 5000.01
The Defense Acquisition System (Cited in para 5–1*b*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8100.02
Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG) (Cited in para 2–5.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8140.01
Cyberspace Workforce Management (Cited in para 2–2*d*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8100.04
DOD Unified Capabilities (UC) (Cited in para 1–1.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited in para 2–2*c*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

IEEE 802.1X
Port Based Network Access Control (Cited in para 2–3*c*.) (Available at http://www.ieee802.org/1/pages/802.1x.html.)

Public Law 107–347
E-Government Act of 2002 (Cited in para 2–5.) (Available at https://www.gpo.gov/fdsys.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 25–30
Army Publishing Program

AR 380–5
Department of the Army Information Security Program

CNSSP 17
Policy on Wireless Systems (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

Defense Information Systems Agency (DISA) DOD Bluetooth Requirement Specifications
(Peripheral Device Security Requirements) (Available at http://iase.disa.mil/stigs/documents/.)

DISA Wireless Security Technical Implementation Guide (STIG) Version 6 Release
(Available at http://iase.disa.mil/stigs/net_perimeter/wireless/pages/index.aspx.)

DODI 5000.02
Operation of the Defense Acquisition System (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8420.01
Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8500.1
Cybersecurity (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

ICD 503
Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation (Available at https://www.dni.gov/files/documents/icd/icd_503.pdf.)

SP 800–53 Revision 4
Security and Privacy Controls for Federal Information Systems and Organizations (Available at https://csrc.nist.gov/publications/pubssps.html.)

SP 800–153
Guidelines for Securing Wireless Local Area Networks (WLANs), (Available at https://csrc.nist.gov/publications/pubssps.html.)

Section III

Prescribed forms
This section contains no entries.

Section IV

Referenced forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (https://armypubs.army.mil/). DD forms are available on the Office of the Secretary of Defense website (https://www.esd.whs.mil/Directives/forms/).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 1494
Application for Equipment Frequency Allocation

Glossary

Section I

Abbreviations

AO
authorizing official

AP
access point

APL
approved products list

AR
Army regulation

BPA
blanket purchase agreement

CHESS
Computer Hardware Enterprise Software and Solutions

CIO
Chief Information Officer

CJCSM
Chairman of the Joint Chiefs of Staff Manual

CNSSP
Committee on National Security Systems Policy

CSA
Cognizant Security Authority

CTTA
Certified Tempest Technical Authority

DA
Department of the Army

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

EAL
evaluation assurance level

ELA
enterprise license agreement

ESI
enterprise software initiative

ESSID
Extended Service Set Identifier

FCC
Federal Communications Commission

FIPS
Federal Information Processing Standard

IdAM
Identity and Access Management

IEEE
Institute of Electrical and Electronics Engineers

IR
infrared

IS
Information system

LAN
local area network

NEC
Network Enterprise Center

NIAP
National Information Assurance Partnership

NIPRNET
Nonclassified Internet Protocol Router Network

NIST
National Institute of Standards and Technology

NSA
National Security Agency

NSI
National Security Information

OSI
Open System Interconnection

PAM
pamphlet

PC
personal computer

PED
portable electronic device

RF
radio frequency

RMF
Risk Management Framework

SAP
Security Authorization Package

SCIF
Sensitive Compartmented Information Facility

SIPRNET
Secret Internet Protocol Router Network

SSID
Service Set Identifier

STIG
Security Technical Implementation Guide

UC
unified capabilities

UCR
unified capabilities requirements

UWB
ultra-wideband

WAP
Wireless Access Protocol

WIDS
Wireless Intrusion Detection System

WLAN
Wireless Local Area Network

WPA2
Wi-Fi Protected Access 2

WPAN
Wireless Personal Area Network

Section II

Terms

Portable Electronic Device
Refers to any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. These include, but are not limited to: laptop computers with wireless capabilities, cellular/personal communication system devices, audio/video/data recording or playback devices, scanning devices, remote sensors, messaging devices, personal digital assistants (PDAs) (for example, Blackberries, Palm Pilots, Pocket PCs), and two-way radios.

Section III

Special Abbreviations and Terms
This section contains no entries.