



Information Assurance Best Business Practice (IA BBP)

U.S. Army CIO/G-6
Cybersecurity Directorate

WIRELESS SECURITY STANDARDS Version 4.0

26 June 2013

WIRELESS SECURITY STANDARDS

Version 4.0

1. Overview:

A. This IA BBP supersedes all previous versions and describes standards for the deployment and use of enterprise wireless network technologies within the Department of the Army (DA). It provides guidance on the protection of Army resources and data from wireless-based security threats, improves incident response techniques for wireless attacks, and mitigates interference among wireless technologies.

B. This document addresses the use and implementation of unclassified Institute of Electrical and Electronics Engineers (IEEE) 802.11 (wireless local area network [WLAN]) and 802.16 (wireless personal area network [WPAN]) devices, systems and technologies.

C. Advances in wireless signaling technology have allowed for increased transmission distances. As a result, our adversaries can utilize unauthorized reception exploitation methods to access and decipher transmitted data which lack the use of encryption and authentication protocols.

D. Exposure of sensitive data is not the only concern for the Army. Websites devoted to open access points (AP) throughout the country are expanding and are likely to include open APs ("hot spots") within the Army span of control. Since wireless network devices operate using radio signals, proliferation of these devices in the Army can lead to Radio Frequency Interference (RFI) amongst radio devices using the same frequency bands. Wireless signals, defined as radio transmissions are susceptible to attacks by suitable, radio interception devices or jammed intentionally by other wireless and/or electromagnetic devices.

2. References:

- A. Army Regulation (AR) 25-2, Information Assurance, 23 March 2009, (http://www.apd.army.mil/pdf/files/r25_2.pdf).
- B. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008, (http://www.apd.army.mil/pdf/files/r25_1.pdf).
- C. AR 5-12, Army Management of the Electromagnetic Spectrum, 1 October 1997, (http://www.apd.army.mil/pdf/files/r5_12.pdf).
- D. IA BBP 07-DC-M-0007, Connection Approval Process (CAP), (<https://informationassurance.us.army.mil>).
- E. IA BBP 06-EC-O-0007, Road Warrior Laptop Security, (<https://informationassurance.us.army.mil>).
- F. DoD Directive (DoDD) 5000.01, The Defense Acquisition System, 20 November 2007, (<http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf>).
- G. DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), 23 April 2007, (<http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf>).
- H. DoDD 8500.1, Information Assurance (IA), 24 October 2002, (<http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>).
- I. DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management, 15 August 2004, (<http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>).
- J. DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, 8 December 2008, (<http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf>).

WIRELESS SECURITY STANDARDS

Version 4.0

- K. DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2009 (<http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf>).
- L. DoDI 8500.2, Information Assurance Implementation, 6 February 2003, (<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>).
- M. DoDI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction, 28 November 2007, (<http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>).
- N. Committee on National Security Systems Policy (CNSSP) No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, 1 October 2012, (http://www.cnss.gov/Assets/pdf/CNSSP_No_2015_minorUpdate1_Oct12012.pdf).
- O. CNSSP No. 17, Policy on Wireless Communications: Protecting National Security Information, May 2010, (<http://www.cnss.gov/Assets/pdf/CNSSP-17.pdf>).
- P. Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems, (<http://www.fas.org/irp/offdocs/dcid-6-3-manual.pdf>).
- Q. Defense Information Systems Agency (DISA) DoD Bluetooth Requirement Specifications [Peripheral Device Security Requirements], 16 July 2010, (http://iase.disa.mil/stigs/net_perimeter/wireless/wireless_pol.html).
- R. DISA Wireless Security Technical Implementation Guide (STIG) Version 6 Release 6, 5 April 2013, (http://iase.disa.mil/stigs/net_perimeter/wireless/wireless_net.html).
- S. National Institute of Standards and Technology (NIST) Special Publication 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs), February 2012, (<http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf>).

3. Point(s) of Contact (POC):

CIO/G-6 Cybersecurity Directorate

Mr. William E. Biggs	william.e.biggs.civ@mail.mil	703-545-1693 (DSN 332)
Mr. Dwayne C. Barrett	dwayne.c.barrett.civ@mail.mil	703-545-1608 (DSN 332)

4. Wireless Security Standards:

This BBP provides best practices and guidance on the implementation and use of wireless technologies within the DA, and leverages applicable Department of Defense (DoD) Directives, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), and DA memorandums and regulations, as referenced.

A. Administrative Requirements:

Implementation of the guidance put forth in this BBP is essential to the security of current and future wireless networks implemented within the Army. Standardized implementation approaches are key to ensuring interoperability and information assurance requirements are met, thus enabling communication across agencies and operating environments.

- (1) **Applicability:** This Wireless Security Standards BBP applies to all wireless networks, systems and devices that are Army owned, controlled, or contracted that process, store, or transmit unclassified information. This BBP does not apply to an information system

WIRELESS SECURITY STANDARDS

Version 4.0

- processing Sensitive Compartmented Information (SCI) or Signals Intelligence Information Systems information. Those information systems must follow processes identified in Director of Central Intelligence Directive 6/3.
- (2) **Designated Approval Authority (DAA):** The DAA appointed in accordance with (IAW) AR 25-2 is responsible for ensuring that all WLAN and portable electronic device (PED) technologies (e.g., smartphones, tablets) at a minimum adhere to the requirements outlined in AR 25-2 and this BBP. For non-compliant wireless implementations, the DAA is responsible for approving and maintaining mitigation plans as part of their acceptable level of risk determination.
 - (3) **Network Enterprise Centers (NEC):** NEC local area networks (LAN) consist of all network enclaves below the top level architecture (TLA) stack to include all tenant installations. NEC offices will identify and monitor all wireless gateways and APs on their enclave network. No wireless devices or networks will operate on the NEC's (LAN) unless they have been approved by the DAA for the installation's networks and the systems are accredited.
 - (4) **Approval to Connect:** All wireless networks and devices must be approved and accredited prior to being approved to operate on the NECs LAN. All unauthorized and unaccredited wireless devices and networks will be rendered inoperable and restricted from use until an approval is granted through the Army's certification and accreditation (C&A) process.
 - (5) **Mitigation Plan:** Currently fielded wireless LAN and PED technologies that are *not* in compliance with this BBP must have mitigation plans developed and submitted to the designated system DAA within 90 days to ensure the systems will meet the requirements of this BBP.
 - (6) **Assessments:** The Information Assurance Manager (IAM) will ensure wireless assessment scans are performed on a monthly basis on their respective ISs through the use of the DoD approved Wireless Discovery Device (WDD) and mapping tool. Scanning reports and logs must be maintained for a minimum of one (1) year.

The Flying Squirrel tool is accessible to Army users via the following link:
(<http://www.nrl.navy.mil/chacs/5545/flyingsquirrel/>).

The Flying Squirrel concept of operations (CONOPS), available at
(<http://www.nrl.navy.mil/chacs/5545/flyingsquirrel/#/doc>), is the Army's guide for all wireless assessment scanning.

B. Wireless LAN Requirements:

- (1) Wireless solutions must be configured to preclude backdoors into the Army's LANs. Backdoors can be caused by either unprotected transmissions or unprotected PEDs entering a network. Systems must also meet all Information Assurance Vulnerability Message (IAVM) compliance requirements.
- (2) Where wireless LANs are to be implemented, a 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 IA personnel can successfully determine these risk factors. IA personnel will have all training documented and meet all training requirements outlined in DoDD 8570.01 (reference i). At a minimum, individuals who conduct risk analysis of wireless networks will have a vendor neutral industry

WIRELESS SECURITY STANDARDS

Version 4.0

standard wireless certification, equivalent to that of a Certified Wireless Network Administrator (CWNA) certification or a Certified Wireless Security Professional (CWSP) certification through the Certified Wireless Network Professional (CWNP) Program, and also contain a thorough understanding of Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

- (3) Fielded wireless LANs and PEDs with connectivity to the GIG must meet the C&A security requirements outlined in DoDI 8510.01 (reference m). Pilot projects must consider and work to meet all wireless requirements per cited references and BBPs.
- (4) 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. Appointed NEC personnel will respond to all WIDS alerts, maintain reports and document actions taken. WIDS logs and documented actions must be maintained for a minimum of (1) year.

C. Component Configuration Requirements:

- (1) Commercial off-the-shelf (COTS) products typically have factory default settings designed for ease of use that do not meet Army security requirements. Wireless equipment must be configured to meet current DoD and Army standards.
- (2) Wireless Access Points (WAP / AP) utilize an Extended Service Set Identifier (ESSID) or Service Set Identifier (SSID) in determining the authorized group of mobile radios. The ESSID/SSID broadcast option must be turned off at the AP.
- (3) Media Access Control (MAC) address filtering must be enabled to prevent unauthorized users access to the network. The (MAC) address is a unique numeric identifier that is programmed into a wireless network interface card (NIC) by the manufacturer. Many manufacturers allow this identifier to be reprogrammed by the user, therefore it must be assumed that the MAC address can be copied electronically (spoofed) and used to gain unauthorized access to a network.

D. Authentication:

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

E. Protection of National Security Information (NSI):

Any wireless solution transmitting data of a National Security nature (i.e. National Security Information [NSI], classified information) must protect data-in-transit with National Security

WIRELESS SECURITY STANDARDS

Version 4.0

Agency (NSA) approved encryption IAW CNSSP No. 15 (reference n), CNSSP No. 17 (reference o), and DoDD 8100.02 (reference g).¹

F. Encryption:

- (1) 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 of AR 25-2, which cites FIPS 140-2 Level 2 compliancy as the end-state requirements for cryptography.
- (2) At a minimum, the IA controls in wireless solutions will have Common Criteria (CC) 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.
- (3) NSA approved Type 1 encryption must be used for any situation requiring protection of classified information.
- (4) Tactical environments must use NSA approved cryptography IAW AR 25-2 Chapter 6. Only under special circumstances will 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 must be approved on a case-by-case basis by HQDA CIO/G-6. Contact the POCs listed in this BBP for further guidance.

G. Bridging, Multi Point, and Point-to-Point Technologies and Topologies:

IEEE publication 802.11 series is the industry standard for WLAN equipment, and is the standard to consider when acquiring WLANs. IEEE 802.3, is a standard that can be used for long distance hi-speed (100Mbs or higher) bridges. If bridges are used, then they must utilize end-to-end encryption using a FIPS 140-2 Level 2 validated cryptographic modules. There is no exception granted when bridges connect into an Army backbone. Wireless Ethernet Bridges (WEB) can generally be categorized by environment (indoor/outdoor), topology (point-to-point, multipoint), and type of technology (802.11b/g, 802.11a, 802.3).

Wireless Metropolitan Area Network (WMAN) solutions, and "last mile" wireless point-to-point bridging solutions using technologies, such as Worldwide Interoperability for Microwave Access (WiMAX) (802.16), Millimeter Wave (MMW), and Free-Space Optics (FSO) require Quality of Service (QoS) protocols to ensure consistent service. OSI Layer 3 or OSI Layer 2 protection using FIPS 140-2 Level 2 encryption schemes must be used with these bridging solutions. Dual Layer protection using NSA certified overlay AES encryption must be implemented to protect data packets on classified or mission critical (tactical) networks.

H. Wireless Personal Area Networks:

¹ Public Law 107-347 defines NSI as data processed by National Security Systems whereby the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or equipment that is an integral part of a weapon or weapons system. It is important to note that information processed by a National Security System can be either classified or unclassified in nature. All NSI requires NSA approved encryption.

WIRELESS SECURITY STANDARDS

Version 4.0

Wireless personal area network (WPAN) communications (e.g., Bluetooth, Zigbee, Ultra Wideband [UWB] and similar technologies) require protection of data-in-transit using either NSA approved Type 1 encryption or FIPS 140-2 validated encryption, as appropriate, unless explicit written approval by the DAA is obtained 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. Example of secure authentication between WPAN devices (e.g., Bluetooth) is outlined in reference (I), which includes some of the following guidelines:

- (1) A randomly-generated PIN of at least 8 decimal digits in length should be used for each pairing.
- (2) The Bluetooth headset/audio gateway device must remain undiscoverable to other Bluetooth devices at all times other than the initial pairing process.
- (3) Bluetooth Security Mode 3 must always be used by the headset and the audio gateway device along with 128 bit Bluetooth encryption.

I. Remote Access:

Mobile users connecting to a commercial wireless service provider must follow the "Road Warrior" Laptop Security BBP to protect data-in-transit, data-at-rest, and the user's PED.

J. Wireless PED Requirements:

Wireless PEDs will be restricted to unclassified two-way wireless data transmission and non-secure voice communication. Wireless PEDs are considered extensions of a LAN environment and must be configured in accordance with the appropriate DISA STIG so that the security posture of the device and the Army network are not compromised. Some Wireless PEDs are equipped with Wi-Fi, Voice over Internet Protocol (VoIP) and Global Positioning System (GPS) functionality.

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 information system (IS) accreditation packages, security policies, security awareness and training, and network user agreements:

- a) Only those applications approved by the cognizant DAA will be approved for use.
- b) PEDs will only be connected to unclassified computers.
- c) PEDs wireless connectivity features (e.g., Wi-Fi, Bluetooth) must not be enabled while the PED is connected to the network, or physically connected to a desktop or laptop, especially a networked personal computer (PC).
- d) Wireless PEDs shall be configured in accordance with the appropriate STIG and applicable System Administrator (SA) Standard Operating Procedures (SOP).
- e) Wireless PEDs must utilize an applicable enterprise server to both enhance security and improve remote management/policy enforcement capabilities.

WIRELESS SECURITY STANDARDS

Version 4.0

- (1) **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 (e.g., 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 the respective facilities, and shall take all physical security steps necessary to prevent introduction of unauthorized devices.

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

- (2) **Accreditation:** Wireless devices such as laptops, PC tablets, and personal digital assistants (PDA) connecting to a network shall be included in the updated DoD Information Assurance Certification and Accreditation Process (DIACAP) process currently established, and signed by the DAA. A thorough and comprehensive requirements validation, risk analysis, and an implementation and migration plan shall be included within the required DIACAP package. Wireless connectivity will not be authorized if the wired infrastructure that is to be extended is not accredited.
- (3) **Authentication:** In no instance will a PED without strong identification and authentication (I&A) be used to store, process, or transmit official Army information. I&A is the process of accepting a claimed identity and establishing the validity of that claimed identity. Strong I&A is identified as two-factor authentication. PEDs without strong I&A built in or added to the system will only be used for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.
- (4) **Encryption:** Web-enabled PEDs that rely on wireless access protocol (WAP) and/or use commercial wireless network providers are at risk for information compromise. Data will not be transmitted 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 (PKI) digital certificates and by allowing customers to run their own WAP gateways for secure, direct connections to web-based resources.
- (5) **Data-at-Rest:** Unless explicit written approval by the DAA is obtained to forgo this requirement, PEDs will fully comply with all mandated data-at-rest (DAR) protection requirements.
- (6) **Anti-Virus:** To ensure consistent levels of protection required against viruses, it is important to maintain up-to-date signature files that are used to profile and identify viruses and 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.
- (7) **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 IAW the same network scanning requirements for wired information systems and devices. For example, vulnerability, compliance, and malware scans using tools such as Retina and QTip. Further guidance and training on network scanning tools is available at (<https://www.acert.1stiocmd.army.mil>) and (<https://iatraining.us.army.mil>).

WIRELESS SECURITY STANDARDS

Version 4.0

K. Wireless Keyboards and Mice:

- (1) Wireless keyboards and mice using radio frequency (RF) protocols (WLAN technologies such as the 802.11-based standards and draft standards; WPAN 802.15-based standards such as Bluetooth, Coexistence, WiMedia, UWB, Zigbee; 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 Type 1 products (if NSI data is processed) are used, and are approved for use by the cognizant DAA in consultation with the Certified Tempest Technical Authority (CTTA).
- (2) Wireless keyboards and mice using infrared (IR) are authorized for use on workstations/servers attached to the NIPRNet or SIPRNet with the approval of the cognizant DAA in consultation with the Certified Tempest Technical Authority (CTTA). The area where the IR is to be used must be totally 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.
- (3) There must 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.
- (4) Any use of compliant RF or IR wireless mice and keyboards in an area that electronically stores, processes, or transmits classified information must be approved by the DAA in consultation with the CTTA.
- (5) 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.

L. Bluetooth:

Commercial Bluetooth wireless headset solutions that do not meet DoD and Army Bluetooth security standards are prohibited by DoD and Army. CIO/G-6 Cybersecurity Directorate is following the progress of a secure Bluetooth Wireless Headset based on specifications provided by NSA and DISA and approved by the DoD Chief Information Office (DoD CIO). Currently, only wired headsets are authorized for use with PEDs.

M. Prohibited Standards and Protocols:

The following standards, technologies, and products are **not** approved for use within the Army.

Note: *Military and civilian personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DoD and Army policies and procedures.*

- (1) **Bluetooth Wireless Headsets:** Users are only permitted to use wired hands-free devices. Both the Bluetooth hands-free and headset profiles are disabled by the wireless push email server security policy configuration.

WIRELESS SECURITY STANDARDS

Version 4.0

- (2) **Wi-Fi Protected Setup (WPS):** The WPS security protocol allows routers and wireless clients to synchronize configuration and security settings in order to simplify the process of connecting to an encrypted wireless network; however, the WPS feature is highly vulnerable to a number of physical and electronic attacks that can result in unauthorized access.
- (3) **Wired Equivalent Privacy (WEP):** The WEP security protocol based on the Rivest Cipher 4 (RC4) encryption algorithm is built into the IEEE 802.11 legacy Wi-Fi standard for WLANs. This standard does not use a FIPS-validated cryptographic module and has been found by the cryptographic community to have fundamental flaws that allow for rapid compromise of the encryption using readily available tools.
- (4) **Wi-Fi Protected Access, Version 1 (WPA):** The WPA security protocol implements the Temporal Key Integrity Protocol (TKIP); however, WPA does not utilize a very strong message integrity check algorithm to verify the packets, which causes it to be especially susceptible to attack.
- (5) **Wi-Fi Protected Access, Version 2 (WPA2):** The WPA2 security protocol uses AES encryption with a 128-bit key strength and the CCMP protocol for strong machine-based authentication; however, without the use of a FIPS 140-2 validated AES encryption module, 802.11i with WPA2 is **not** approved.

Note: AES encryption modules are not FIPS 140-2 validated by default. Only AES encryption modules that have been validated by NIST and are listed on the NIST FIPS 140-2 validated modules website (<http://csrc.nist.gov/cryptval/140-2.htm>) are considered to be approved for use within the Army.

5. Training:

All users being issued a PED must complete security awareness training regarding the physical and information security 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.

6. Products:

- 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 the Military Communications Electronics Board (MCEB) per DoDD 5000.1 and AR 5-12. If you have a new solution not previously considered by the MCEB you must submit a spectrum supportability requests DD-1494 to the Army Spectrum Management Office, ATTN: Arthur Radice, 2461 Eisenhower Avenue, Alexandria, VA 22331-2200.
- C. Only approved IA products will be acquired and used. Approved products are listed on the DoD Unified Capabilities (UC) Approved Products list (APL) (<https://aplits.disa.mil>); listed as approved in the latest IA BBPs (<https://informationassurance.us.army.mil>); or specified as approved in current, signed CIO/G-6 issuances. Army customers who wish to have IA or IA-enabled products considered for the DoD UC APL must contact the Army CIO/G-6 Cybersecurity Directorate to coordinate sponsorship.
- D. Products must be procured through the Army Computer Hardware Enterprise Software and Solutions (CHESS) program. Products not available through CHESS may be purchased using an

WIRELESS SECURITY STANDARDS

Version 4.0

existing DoD Enterprise License Agreement (ELA) or DoD Blanket Purchase Agreement (BPA), such as via the DoD Enterprise Software Initiative (ESI). Products listed on CHES 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 (CoN), as required.



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

SAIS-CB

26 JUN 2013

MEMORANDUM FOR ALL ARMY ACTIVITIES

SUBJECT: Implementation of the Information Assurance Best Business Practice (IA
BBP) Number 09-EC-M-0010

As the Director, Army CIO/G-6 Cybersecurity Directorate, and the Army FISMA Senior IA Officer (SIAO), the undersigned approves the revised Wireless Security Standards IA BBP, version 4.0, 09-EC-M-0010, in support of Army Regulation 25-2 and the Army Information Assurance Program (AIAP). This BBP reflects the current standards to be implemented throughout the Army for all information systems and networks for the identified purpose.

Encl

A handwritten signature in black ink, appearing to read "Stuart M. Dyer".

STUART M. DYER
Major General, GS
Director, CIO/G-6 Cybersecurity