WIRELESS SECURITY STANDARDS
VERSION 3.0

1. Overview

A. This supersedes all previous versions and establishes standards for the deployment and use of 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 Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless local area network (WLAN) devices, systems and technologies, capable of processing, storing and transmitting data at the unclassified level. This also includes guidance on the implementation of 802.16 based technologies and the implementation of wireless personal area networks (WPAN).

C. Advances in wireless signaling technology have allowed for increased transmission distances. As a result, our adversaries have increased standoff capabilities utilizing unauthorized reception exploitation methods. Without the use of encryption and authentication protocols, transmitted data can be read and deciphered by unintended recipients in a matter of seconds.

D. Exposure of sensitive data is not the only concern for the Army. Web sites 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. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008 (URL LINK)
B. AR 25-2, Information Assurance, numerous paragraphs. (URL LINK)
C. AR 5-12, Army Management of the Electromagnetic Spectrum, 1 October 1997 (URL LINK)
D. System Administrator (SA) Standard Operating Procedure (SOP) For BlackBerry, (URL LINK)
E. DoDD 8500.1 Information Assurance (IA), 24 October 2002 (URL LINK)
F. DoDI 8500.2, Information Assurance Implementation, 6 February 2003 (URL LINK)
G. DoDD 5000.1, The Defense Acquisition System, 12 May 2003 (URL LINK)
H. DoDI 8510.01 - Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction, Nov. 28, 2007(URL)
I. DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management, 15 August 2004 (URL)
J. DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 23 April 2007 (URL LINK)
K. DISA Wireless STIG Version 5, Release 2, 15 November 2007 (URL LINK)
L. DISA DoD Bluetooth Headset Security Requirements Matrix, Version 2.0 (URL LINK)
M. DISA DoD Bluetooth Smart Card Reader Security Requirements Matrix, Version 2.0 (URL LINK)

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

NETCOM OIA&C Directorate

Ms. Phyllis Bailey (DAC) phyllis.bailey@us.army.mil 703-602-7408 DSN 332
Ms. Erika Davis (CTR) erika.b.davis@us.army.mil 703-602-8346 DSN 332

WIRELESS SECURITY STANDARDS
VERSION 3.0

Mr. Tim Hiligh (CTR) timothy.hiligh@us.army.mil 703-602-7509 DSN 332

4. Related BBPs (URL)
06-EC-O-0008: Data-At-Rest (DAR) Protection BBP Version 1.0
06-EC-O-0007: "Road Warrior" Laptop Security BBP Version 1.2
07-DC-M-0007: Connection Approval Process (CAP) Version 1.1

5. Description: This BBP provides best practices and guidance on the implementation and use of wireless technologies within the DA, and leverages several 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 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 information systems (IS) processing Sensitive Compartmented Information (SCI) or Signals Intelligence Information Systems (IS) information. Those ISs 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, 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) **Directorate of Information Management (DOIM).** DOIM local area networks (LAN) consist of all network enclaves below the top level architecture (TLA) stack to include all tenant installations. DOIM offices will identify and monitor all wireless gateways and APs on their enclave network. No wireless devices / networks will operate on the DOIM's (LAN) unless they have been approved by the DAA for the installation network 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 DOIMs 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**. Appointed IASOs 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. The Flying Squirrel (FS) tool is accessible to Army users via the Army's Asset and Vulnerability Tracking Resource site, (https:\\avtr.us.army.mil). The FS concept of operations (CONOPS) (available at: https://avtr.us.army.mil/Modules/default.aspx),

will be the Army's standard operating procedure (SOP) for all wireless assessment scanning. Scanning reports and logs will be maintained for a minimum of (1) year.

B. **Wireless LAN Requirements**

(1) Wireless solutions will be engineered 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 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 FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

(3) Fielded wireless LANs and PEDs with LAN connectivity must meet the C&A security requirements outlined in reference (H). 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 DOIM personnel will respond to all WIDS alerts, maintain reports and document actions taken. WIDS logs and documented actions will 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 will 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 will be turned off at the WAP.

(3) Media Access Control (MAC) address filtering will 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]) must protect data-in-transit with National Security Agency (NSA) Type 1 products IAW public law 107-347.

***Note**: 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 certified Type 1 protection.*

F. **Encryption**

(1) All wireless implementations must provide for end-to-end encryption of data-in-transit through the use of validated and approved 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. The NSA approved Type 1 encryption must be used for any situation requiring protection of classified or unclassified NSI IAW AR 25-2 Chapter 6, NSA approved cryptography must be used in a tactical environment.

(3) Only under special circumstances will 802.11 with National Institute of Standards and Technology (NIST) approved FIPS 140-2 Level 2 validated cryptographic modules be used in a tactical environment. These exceptions will be approved on a case-by-case basis by HQDA CIO/G-6. Contact the POCs listed in this BBP for further guidance regarding exceptions.

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

(1) 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).

(2) 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 may be used with these bridging solutions. Dual Layer protection using NSA certified overlay AES encryption will be implemented to protect data packets on classified or mission critical (tactical) networks.

H. **Wireless Personal Area Networks**

Personal area network (PAN) capabilities including Bluetooth, Zigbee, Ultra Wideband (UWB) or any similar technologies require protection of data-in-transit using either NSA Type 1 mechanisms or FIPS 140-2 validated mechanisms, as appropriate, unless explicit written approval by the DAA is obtained to forgo required NSA or FIPS mechanisms. Non-NSI wireless PAN solutions must use a FIPS 140-2 Level 2 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 (H) and (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.

J. **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.

K. **Wireless PED Requirements**

(1) Two-way wireless e-mail devices (TWED) will be restricted to unclassified two-way wireless data transmission and non-secure voice communication. TWEDs 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 TWEDs are equipped with Wi-Fi, Voice over Internet Protocol (VoIP) and Global Positioning System (GPS) functionality.

(2) 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 local DAA will be approved for use.
b) PEDs will only be connected to unclassified computers.
c) A PEDs’ remote connectivity features (i.e. WLAN, Bluetooth, etc.) will not be used while it is connected to the network, or physically connected to a desktop or laptop, especially a networked personal computer (PC).
d) TWEDs shall be configured in accordance with the appropriate STIG and applicable System Administrator Standard Operating Procedures (SA SOP).
e) TWEDs must utilize an applicable enterprise server to both enhance security and improve remote management/policy enforcement capabilities.

(3) **Physical Security**. PEDs with wireless communication capabilities will not be permitted inside sensitive compartmented information facilities (SCIF), classified, or restricted areas, unless, as a minimum, the device’s infrared (IR) port has been completely covered by metallic tape, and/or its transmission capability (i.e. antenna) has been removed or physically disabled. (Note: removal or altering PEDs in this manner may invalidate the warranty of such an item. Please check with the manufacturer before proceeding.) 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.

(4) **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.

(5) **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.

(6) **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.

(7) **Data-at-Rest**. PEDs will fully comply with all mandated data-at-rest (DAR) protection requirements.

(8) **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.

N. **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 **<u>not authorized</u>** 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 local DAA.

(2) Use of IR wireless keyboards and mice are authorized for use on workstations/servers attached to the NIPRNet or SIPRNet with the approval of the local 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 (i.e. if IR is used on a classified device, all IR ports on unclassified devices must be disabled

using metallic tape. If IR is used on an unclassified device, all IR ports on classified devices must be disabled using metallic tape). 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.

O. **Bluetooth:** Currently, there are no commercial Bluetooth wireless headset solutions that meet DoD and Army Bluetooth security standards, and use of these devices is prohibited by DoD and Army. Office of Information Assurance and Compliance (OIA&C) Common Access Card (CAC)/PKI is following the progress of a secure Bluetooth Wireless Headset based on specifications provided by NSA and DISA and approved by the Office of the Assistant Secretary of Defense for Networks and Information Integration ASD (NII). Until that solution is available, only wired headsets are authorized for use with TWEDs.

P. **Prohibited Standards and Protocols**

The following standards, technologies and products, are **NOT** approved for use within the Army**:**

(1) **Wired Equivalent Privacy, (WEP)**. The WEP security protocol is based on 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.

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

(3) **Wi-Fi Protected Access (WPA) Version 1.** WPA2 uses AES encryption with a 128-bit key strength. WPA2 also adds 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 modules that have been validated by NIST and are listed on the NIST validated modules website (http://csrc.nist.gov/cryptval/140-2.htm) are considered to be approved for Federal use IAW FIPS 140-2.*

6. 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 the use of the device. This information will be included in the Acceptable Use Policy.

7. Products. Products not listed on the Army Information Assurance Approved Products List (AIAAPL) are prohibited for use within the Army. All IA tools used by the Army must be listed on the AIAAPL prior to acquisition. (https://informationassurance.us.army.mil/ia_tools/IAProducts.xls).

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 5000.1and 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 Alexandria, VA. 22331-2200.

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

Office, Chief Information Officer / G-6

NETC-EST-I

JAN 0 2 2009

MEMORANDUM FOR All Army Activities

SUBJECT: Implementation of Information Assurance Best Business Practice (IA BBP)

As the Director, Army Office of Information Assurance and Compliance and the Army FISMA Senior Information Assurance Officer (SIAO), the undersigned approves the identified IA BBP(s) in support of Army Regulation 25-2 and the Army Information Assurance Program (AIAP). The BBP is the standard to be implemented throughout the Army for all information systems and networks for the identified purpose.

09-EC-M-0010; Wireless Security Standards, Version 3.0

LeRoy Lundgren

LeRoy Lundgren
Director, Army Office of Information
Assurance and Compliance