

# WIRELESS SECURITY STANDARDS (VERSION 1.25)

## 1. Overview

A. This document establishes best practice standards for the deployment and use of local wireless network technologies for the Department of the Army. It intends to protect Army resources and data from security threats, improve incident response for wireless issues, and mitigate interference among wireless technologies. Wireless network devices offer a simple, convenient, and inexpensive solution to extend local area network (LAN) accessibility by reducing the requirements of physical infrastructure. Wireless networking removes the encumbrance of wire connections on portable devices, and can also enable laptop and handheld users the ability to travel beyond traditional network boundaries (e.g. between buildings) without losing network connectivity. This flexibility however, introduces several unique vulnerabilities in addition to the inherent risks associated with any wired network.

B. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, jammed intentionally by other devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including orders to execute, research correspondences, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception that increases the standoff capabilities of our adversaries.

C. Exposure of sensitive data is not the only concern for the Army. If improperly implemented, a wireless network allows an unauthenticated or unauthorized user an internal Army IP address with all the benefits offered to any authenticated user. Using one of these trusted IP addresses; attacks could be launched against the Army or any outside network accessible through the Army's infrastructure. Web sites devoted to open access points throughout the country are expanding and are likely to include open access points ("hot spots") within the Army. Since wireless network devices operate using radio signals, their proliferation in the Army can lead to Radio Frequency Interference (RFI) among these and other radio devices using the same frequency bands. This Best Business Practice (BBP) serves as the foundation for a comprehensive risk mitigation strategy; enhanced by published security standards and, where applicable, a more granular IA specific standard.

### References:

AR 25-2, Information Assurance (PARAs: 1-4c(1); 5-4) ([URL LINK](#))

DoDD 8500.1 Information Assurance (IA) ([URL LINK](#))

DoDI 8500.2, Information Assurance Implementation ([URL LINK](#))

DoD 5200.40I DITSCAP Instruction ([URL LINK](#))

DoD 5200.40M DITSCAP Manual, ([URL LINK](#))

DoDD 8100.2 Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG). ([URL LINK](#))

## 2. IA BBP Point(s) of Contact (POC):

NETCOM IA Directorate; NETC- EST-A

Mike Wanklyn

703-602-7452

mike-wanklyn@us.army.mil

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

**3. Description of Former State:** Army Regulation (AR) 25-2 replaced AR 380-19 which provides for general guidance when considering wireless to traditional WAN / LAN topology. AR 25-2 also rescinded HQDA Ltr 25-02-1 U.S. Army Wireless Policy dated 15 April 2002.

**4. Description of Changes Instituted:** Army Regulation (AR) 25-2 augmented by this Wireless Best Business Practice (BBP).

**5. Description of End State:** Reduced threats associated with the use of wireless networks and associated devices through a three-tier approach.

A. Tier one will consist of multilevel awareness training, which will focus on management, user, and technical personnel.

B. Tier two will use technical solutions from approved vendor sources. These solutions can be hardware or software derived.

C. Tier three will use procedural security.

When an approved device goes outside of the Army's infrastructure i.e. temporary duty (TDY), these devices shall be scanned for malicious code prior to reconnection or when connected to any Army's LAN. This procedure can, and should be automated through the use of scripts. Additionally when connecting to non-parent installations users should have in their possession the certification and accreditation (CA) documentation for their mobile computing device (MCD). The servicing Directorate of Information Management Office (DOIM) may request proof of certification.

**6. Description of Required Resources:** None

**7. Description of Derived Benefits Resulting from Implementation:** Reduction of threats associated with wireless networks, rapid deployment, cost effective, and mobility.

**8. Administrative Requirements:**

A. The command designated approval authority (DAA), appointed in accordance with (IAW) AR 25-2 is responsible for ensuring that all wireless local area networks (LAN) and portable electronic devices (PED) technologies, as a minimum, adhere to the requirements outlined in AR 25-2 and this BBP.

B. Currently fielded wireless LAN and PED technologies that are not in compliance with this BBP must have migration plans developed within four months to ensure the systems will meet the requirements of this BBP. For non-compliant wireless implementations, the DAA is responsible for approving and maintaining these migration plans as part of their acceptable level of risk determination. Any wireless LAN not in compliance and connected to an Army network processing sensitive but unclassified information should be immediately disconnected until approved.

C. Respective Directorate of Information Management (DOIM) offices should identify and monitor all wireless gateways and access points. They should have the ability to run wireless Intrusion Detection Systems (IDS) and be able to perform assessment scans to locate authorized and rogue access points (AP). No one should have the ability to stand up and run a wireless access point unless the DOIM has approved and the systems are accredited.

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

### 9. Related BBPs:

- A. Published BBPs are at: <https://informationassurance.us.army.mil/bbp/>
- B. Draft BBPs are at: <https://www.us.army.mil/portal/jhtml/FileLoader.jhtml?kcid=585383>

**10. Products:** The IA Directorate is working with CLSA, to put wireless solutions on the approved CLSA products list. Check this list often, as changes will occur frequently.

### 11. Description:

#### A. Wireless LAN Requirements:

(1) Pilot and fielded wireless LANs and PEDs with LAN connectivity must meet the same certification and accreditation security requirements as a wired LAN Information Systems (IS) per the cited references. Pilot projects must consider the following requirements during the development of the system:

(2) The following information applies to all current wireless standards including 802.11a (Standard), 802.11b (Standard), 802.11d (Draft), 802.11e (Draft), 802.11f (Draft), 802.11g (Draft), 802.11h (Draft), and 802.11i (Draft). The 802.11i standard promises better security enhancements, using 802.1x authentication mechanisms, and AES encryption, but the Institute for Electrical and Electronic Engineers (IEEE) community has not approved the draft standard for use at this time.

(3) Wireless solutions will be engineered to preclude backdoors and trapdoors into the Army's LANs. Backdoors can be caused by either unprotected transmissions or unprotected PEDs entering a network. Trapdoors can be caused by improperly hardening of platform systems. Systems must meet all Information Assurance Vulnerability Message (IAVM) compliance requirements. Consideration of all factors must be evaluated in the design of a wireless solution.

(4) Commercial off-the-shelf (COTS) products typically arrive with factory default settings that may not offer appropriate security. Wireless equipment that connects to a LAN will be configured for acceptable LAN security options.

(5) IEEE publication 802.11 series is the industry standard for wireless LAN equipment, and is the standard to consider when acquiring wireless LANs. 802.3, is a standard that can be used for long distant hi-speed (100mbs or higher) bridges. If bridges are put in place they must utilize end-to-end encryption using a FIPS 140-2 level 2 validated crypto module. There is no exception to be 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). Just about any combination of topology, technology and environmental application can be found. Most indoor applications utilize the 802.11b or 802.11g standards and are utilized to extend the wireless network, particularly into areas where wired network capability does not exist. These devices range from being Wireless Access Point (WAP) devices set to "bridge only" to dedicated bridging devices. The range of most of these devices is limited to the normal 802.11 b/g range of about three hundred feet. However, users became more demanding of 802.11b/g-based systems and the range was extended by either increased power or by utilization of a focused antenna system. In these configurations, users were looking to interconnect buildings or limited backhaul connection between local sites. Depending on the antenna configuration these devices support either multipoint or point-to-point communications. As technology has progressed, WEBs are now being used over long distances, up to 40 miles, to inter-connect remote sites and to support remote

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

sensor mechanisms (i.e. traffic cameras; security video feeds; highway emergency support, etc). Many of these devices are utilizing an 802.11b based line-of-sight systems. New 802.11a based systems are also being introduced as wireless bridges, which support point-to-point linkages at 54 Mbps at ranges up to seven miles.

(6) Where wireless LANs are to be implemented, thorough analysis, testing, and risk assessment must be done to determine the risk of information intercept/monitoring and network intrusion prior to installation of these devices. It should be noted that only properly trained personnel could successfully determine these risk factors. As a minimum recommendation, persons who conduct this type of risk analysis should have acquired a vendor neutral industry standard wireless certification. Certified Wireless Network Administrator (CWNA) or Certified Wireless Security Professional (CWSP) are examples of acceptable certifications.

(7) Ensure that a user cannot enter a wireless LAN without strong authentication. As a minimum, strong authentication will include extended service set identifier/service set identifier (ESSID/SSID) and media access control (MAC) address identification with an integrity lock. MAC address resolution alone does not qualify as strong authentication.

(8) ESSID/SSID is a common access number/code that is applied to a wireless access point during configuration and with associated wireless network interface cards so access points can identify an authorized group of mobile units. **Make sure that the ESSID/SSID broadcast option is turned off at the access point!**

(9) The MAC address is a unique numeric identifier that is programmed into a wireless network interface card by the manufacturer. Some 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 AIS.

(10) All Army situations where wireless solutions are implemented must fully meet IA requirements. These requirements for a wireless solution as extensions to a LAN environment are as follows.

(11) Wireless devices such as Laptops, PC Tablets, and PDAs connecting to a network shall be included in the updated Certification and Accreditation (DITSCAP) DoD 5200.40I and DoD 5200.40M process already established, and signed by the DAA. A thorough and comprehensive requirements validation, risk analysis, and an implementation and migration plan shall be part of the System Security Authorization Agreement (SSAA) Certification and Accreditation (C&A) update. No wireless connectivity will be authorized if the wired infrastructure that is extended is **not** accredited.

(12) Standards for wireless devices shall meet the requirements of AR 25-2, Information Assurance. AR 25-2 cites FIPS 140-2 level II compliancy as the end-state, for cryptography, in wireless connectivity. Vendors cannot achieve this capability in sufficient time to meet current wireless requirements, but many are engineering solutions that will eventually meet this requirement.

(13) IA standards for wireless connectivity will be as follows until Level II requirements are achieved. Interim products approved for use shall meet the following minimum-security standards to secure the connection and the transmission of data. All interim products acquired will have a migration plan prepared to the approved standard once designed and identified, signed by the DAA. These interim standards are non-waiverable.

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

(a) If the wireless solution considered is based on a software encryption solution, the vendor must demonstrate that they are on the NIST site and are actively pursuing FIPS 140-2 level II certification. At the time of consideration the software encryption solution at a minimum shall be pre-certified to FIPS 140-2 Level I. The wireless solution whether it is from a single source (vendor) solution, or a multiple source (vendor) solution, shall include Layer 2 (data link-layer OSI Model) encryption protection. Encryption strength will be 3DES or AES as a minimum.

(b) In order for hardware or firmware-based encryption solutions to be considered, the vendor must demonstrate that they are on the NIST site and are actively pursuing FIPS 140-2 level II certification. At the time of consideration the firmware-based encryption solution at a minimum shall be pre-certified to FIPS 140-2 Level I. The wireless solution whether it is from a single source (vendor) solution or a multiple source (vendor) solution shall include Layer 2 (data link-layer OSI Model) encryption protections. Encryption strength will be 3DES or AES as a minimum.

(c) Recommend that a requirement be included in all negotiated contracts that will upgrade the wireless solution at no additional cost to the government once the vendor achieves FIPS 140-2 level II. This should include changes to software, hardware, and processors.

(14) Wireless devices used to extend LAN environments shall: support and incorporate all NIAP certified IA related security software, have a host-based firewall, an approved anti-virus product installed, a management client or application, and require user-unique authenticated access to the device as absolute minimums. If the wireless device cannot support the minimum standards it is prohibited from use. This standard is non-waiverable.

(15) At a minimum the wireless solutions being considered should also have a common criteria evaluation rating of EAL 2. EAL 4 is highly recommended and will be the Army end-state requirement. The National Security Agency (NSA) approved type 1 encryption must be used for any situation requiring protection of classified information. SecNet 11 is the only approved solution using the 802.11 standard and is cleared for secret and below. In accordance with AR 25-2 Chapter 6, NSA approved type 1 encryption must be used in a tactical environment. Therefore the only approved solution for 802.11 in a tactical environment is SecNet 11. There are other wireless devices using type 1 encryption, but the NSA has not evaluated or endorsed these products. If such a device is being considered you must contact the HQDA, CIO/G-6 NETCOM IA DIRECTORATE prior to its use or fielding. Only under special circumstances will 802.11 with NIST approved FIPS 140-2 level 2 validated crypto modules be used in a tactical environment. These exceptions will be approved on a case-by-case basis by the office of HQDA CIO/G-6 NETCOM IA DIRECTORATE.

(16) **The following standards are NOT approved for Army use!** Wired Equivalent Privacy, (WEP) a security protocol based on RC4 encryption algorithm, is built into the IEEE 802.11 standards for wireless LANs. This standard does not use a FIPS-validated crypto module, and has been found by the cryptographic community to have fundamental flaws. Wi-Fi Protected Access version 1, (WPA) is a newer security protocol built into the 802.11i (Draft) standard. It offers better protection using temporal key integrity protocol (TKIP). This protocol was added, so that keys are rotated and encryption is strengthened, but it is still based on the RC4 encryption algorithm. WPA2 version 2 of WPA will use strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes). WPA2 also adds two strong authentication features: wireless robust authentication protocol or (WRAP), counter with cipher block chaining message authentication code protocol or (CCMP). The NSA is evaluating AES 256 bit key size for Top

## **WIRELESS SECURITY STANDARDS (VERSION 1.25)**

Secret. Should this occur, FIPS could very well certify 802.11i-using WPA2 AES to FIPS 140-2 standards. As of this time,

(17) Those implementing wireless LANs must include additional security measures for data confidentiality and network intrusion protection, such as the use of Virtual Private Network (VPN) gateways that use validated FIPS 140-2 level 2 cryptographic modules.

(18) Those planning wireless LAN solutions must consider the migration to more secure wireless LAN technologies, which could mean costly replacement of wireless equipment. Careful research is required. Don't buy equipment unless you have a maintenance contract in place that will allow for replacement or upgrade to the equipment when the newer wireless security technologies are made available or are mandated.

### **B. Wireless PED Requirements:**

(1) As technology advances, approved anti-virus software for PEDs will be available. 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.

(2) PEDs, other than approved laptop computers, will not be used for classified information processing. PEDs do not currently provide adequate security mechanisms to protect classified data from compromise.

(3) PEDs with wireless communication capabilities will not be permitted inside sensitive compartmented information facility (SCIF), classified, or restricted areas, unless, as a minimum, the device's infrared port has been completely covered by an opaque tape (black electrical tape or 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.)

(4) 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 facilities, and shall take all physical security steps necessary to prevent introduction of these devices. (See Joint DoDIIS/Cryptologic Sensitive Compartmented Information (SCI) Information Systems Security Standards, Chap 15.) The various wireless and wired interconnection capabilities, and multi-capable functioning of the PEDs presents a significant risk that classified or sensitive information will be compromised over an unclassified medium. Technologies exist that can actively disable wireless capabilities within restricted areas and are recommended in sensitive, restricted, or critical areas.

(5) In no instance will a PED without strong identification and authentication (I & A) (that is, login and password/pin) be used to store, process, or transmit official Army information. 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) The DoD public key infrastructure (PKI) and digital certificates will be used to the greatest extent possible to support security solutions for user identification and authentication, data confidentiality (using FIPS-validated crypto modules), and non-repudiation when using PEDs for wireless communications. Security solutions using digital certificates must comply with DoD PKI requirements. When external certificate authorities are necessary, issuance of certificates plans for key escrow, and revocation of user certificates must be documented.

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

(7) Personal Area Networks (PAN) (including Bluetooth) will not be utilized for transmitting sensitive information unless the data is encrypted with FIPS 140-2 level 1, with demonstrated movement towards level 2, validated crypto module. There is no known inherent security planned for Bluetooth (802.15) therefore it should not be used as the sole mechanism for transmission of unencrypted Army data, not even to a printer. The print job can be intercepted if you are using only Bluetooth. Normally PAN devices including Bluetooth operate at a distance of 30 feet or less. Newer Bluetooth devices on the market can now transmit up to 300 feet. No Army information should be sent in the clear using PAN technology unless secured using approved FIPS validated encryption.

(8) 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-validated crypto module. The WAP standard is evolving to support data confidentiality requirements through the use of PKI digital certifications and by allowing customers to run their own WAP gateways for secure, direct connections to web-based resources.

(9) When WAP gateways are installed in the top-level architecture (TLA) of Army installation networks to provide access to web-servers, they will be properly controlled and monitored by firewalls and intrusion detection systems (IDS) as a minimum.

(10) The use of any wireless device, including commercial unlicensed devices, must be coordinated with the local Army frequency manager prior to purchase. Use of wireless devices may not be approved for use in another country, since each country allocates its frequency resources differently.

(11) 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 Alexandria, VA. 22331-2200. The DD-1494 will be reviewed by Mr. Radice before they are sent to the 17-agency committee that meets monthly. The process usually will take up to six months so plan accordingly.

(12) All users being issued a PED must be provided security awareness training regarding the physical and information security vulnerabilities of the device and include this information in the Acceptable Use Policy.

(13) Army commands and activities whose members use PEDs that synchronize with desktop or laptop computers on the Army networks will adopt the following security measures and write them into the command IS security policies, security awareness and training, and network user agreements:

- (a) Only use applications that are approved by the local DAA.
- (b) PEDs will only be connected to unclassified computers.
- (c) Passwords, combinations, personal identification numbers (PIN) and classified information will not be stored on PEDs.
- (d) Do not use a PEDs' remote connectivity features (i.e. wireless) while it is physically connected to a desktop or laptop personal computer (PC), especially a networked PC, or otherwise connect to the network.

(14) Two-way wireless email devices, such as BlackBerries, are capable of two-way unclassified wireless transmission and reception. They are **not** considered as extensions of a

## WIRELESS SECURITY STANDARDS (VERSION 1.25)

LAN environment. These devices' functionality is restricted to text messaging capabilities only. Though some units support voice capability as well, it is important to remember that it is strictly non-secure. Some additional guidance follows:

- (a) As with other PEDs, two-way wireless email devices must use FIPS 140-1/2 validated cryptographic modules and NIST-approved cryptographic algorithms (3DES or AES only).
- (b) When using multiple BlackBerries on a network, the use of a BlackBerry Enterprise Server (BES) is strongly encouraged, both to enhance security and to improve remote management/policy enforcement capabilities (whenever local IT budget and infrastructure can support).
- (c) No anti-virus capability currently exists on the BlackBerry handheld itself. The risk of a Java-based virus causing harm to the handheld is currently minimal to non-existent. In the meantime, the anti-virus function will continue to be performed at the exchange server and the desktop.
- (d) No capability for encryption of data at rest currently exists (other than data deliberately encrypted with DoD PKI). This feature is expected to become available as part of the release of BlackBerry Desktop 4.0.

### **C. Standards for implementing wireless LANs.**

(1) Wireless solutions must be certified to FIPS 140-2 level 1 end-to-end encryption. Triple DES or AES are the only acceptable standards. Vendors must demonstrate movement to FIPS 140-2, Level 2 certification for continued use.

(2) Wireless solutions must protect layer two (link layer OSI model) with an approved FIPS 140-2 level 1 encryption module. Vendors must demonstrate movement to FIPS 140-2, Level 2 certification for continued use.

(3) Wireless solutions must be able to detect and suppress rogue access points. Set up access controls to only allow authorized devices and users access to the wireless network.

(4) Wireless solutions must incorporate a location aware protection scheme, i.e., security policies are enforced based on location, connection interface (e.g., PCMCIA card), and wireless access points. *This measure is for both home and traveling.*

### **D. Standards for mobile wireless computing "Road Warrior"**

(1) Mobile devices must have a VPN client configured to establish a secure tunnel. Reason: Layer 2 cannot be protected with current technology unless we own the network. VPN's operate at layer 3, helping to mitigate, but not eliminate, layer 2 risks. VPNs must meet encryption certification requirements, i.e., FIPS 140-2 level 1. Vendors must demonstrate movement to FIPS 140-2 level 2, before authorization to use.

(2) Mobile devices must have an EAL 4 + approved firewall configured to only allow authorized communications. Firewall must operate at the Network Driver Interface Specification (NDIS) Layer using stateful packet inspection.

## **WIRELESS SECURITY STANDARDS (VERSION 1.25)**

(3) Mobile devices must have a crypto solution loaded that safeguards data at rest and not allow unauthorized user access or alteration.

(4) Wireless solution must incorporate a location aware protection scheme, i.e., security policies enforced based on location, connection interface (e.g. PCMCIA card), and wireless access points.

(5) Mobile devices must have an Army authorized anti-virus products installed

(6) Mobile devices should include, in addition to the basics IA requirements above, additional IA enabling software and configuration for data and OS protection as technology is available (i.e. OS wrappers, disk partitioning, tamper evident seals, disk-wiping software in the event of loss or illegal access).

(7) This BBP will be supplemented with additional guidance and acceptable standards in a BBP specifically addressing traveling laptop configurations and security measures.

### **E. Factors affecting poor wireless implementation**

(1) A significant security factor associated with the proper use of wireless technologies and, in particular, PEDs is the acknowledgement by the user that the PED is, in fact, functioning in the same capacity as a standard PC or workstation: therefore, it is subject to the same regulations. Reinforcing the standard information security training and discussion of the Army's Defense In Depth Program as part of this training can help to raise user awareness of the vulnerabilities associated with these systems. The Defense In Depth Program is a security strategy endorsed by the Army as a means to counter security vulnerabilities.

(2) The following characteristics/limitations of wireless solutions must be considered prior to their use:

(a) Wireless solutions will create backdoors into Army LANs if not implemented properly. If a device receives information via a wireless technology and that device allows that information to be placed directly into the LAN at the workstation level, then all perimeter and host-based security devices have been bypassed.

(b) Wireless LANs are susceptible to interference, interception, and jamming. Again if not implemented properly, an attacker can jam an access point (AP) causing a denial of service condition, which will prevent the user from connecting. Another methodology is to use a well-documented DOS attack that will redirect users to an established rogue access points. There is no known fix to either of these scenarios because of 802.11 engineering. If the condition is not addressed, hot points could be established all along the Army's backbone. For these situations, VPNS are recommended between remote users and Army controlled access points to protect the confidentiality of the session and data. Remote user devices such as laptops should have VPN clients and personal firewalls loaded before the remote device can be used. Accreditation of these remote devices is a must under current DITSCAP DoD 5200.40I and DoD 5200.40M.



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

JUN 22 2004

Office, Chief Information Officer / G-6

NETC-EST-IAD

MEMORANDUM FOR All Army Activities

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

As the Army Information Assurance Director, the undersigned approves the following IA BBP to support the Army Information Assurance Program (AIAP). The BBP will be implemented throughout all information systems and networks as applicable, as the Army standard for IA implementation for the identified purpose.

**04-EC-M-0003: Wireless Security Standards; Version 1.25**

A handwritten signature in black ink, appearing to read "Thaddeus A. Dmuchowski".

Thaddeus A. Dmuchowski  
Colonel, GS  
Director, Information Assurance