DEPARTMENT OF THE ARMY
WASHINGTON, D.C. 20310

HQDA Ltr 25-02-1

SAIS-IOA

15 April 2002

Expires 15 April 2004

SUBJECT: U. S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy

SEE DISTRIBUTION

1. **Purpose.** This letter provides policy for the acquisition and use of wireless communication solutions and portable electronic devices (PED) (data enabled cellular phones, two-way pagers, personal digital assistants (PDA), and handheld/laptop computers with wireless connectivity capabilities).

2. **Applicability.** This policy applies to the Active Army, the Army National Guard of the United States, and the United States Army Reserve.

3. **Proponent and exception authority.** The proponent of this letter is the Chief, Information Officer, G-6 (CIO/G-6). The proponent has delegated exception authority to the Director of Information Assurance (SAIS-IOA) for all matters pertaining to Army networks security.

4. **References.**

a. Required publications.

(1) Army Regulation 5-12, Army Management of Electromagnetic Spectrum.

(2) Army Regulation 25-1, Army Information Management.

(3) Army Regulation 380-I 9: Information Systems Security.

(4) Army Regulation 380-53: Information Systems Security Monitoring.

(5) Department of Defense Directive 5000.1: Defense Acquisition System. Available at: http://www.dtic.mil/whs/directives.

(6) Department of Defense Instruction 5200.40: DOD Information Technology Security Certification and Accreditation Process (DITSCAP). Available at: http://www.dtic.mil/whs/directives.

(7) Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (rev. 2). Available at: http://www.fas.org/irp/doddir/dod/jdcsisss-rev2.htm.

b. Related publications.

Printed on Recycled Paper

(1) Institute for Electrical and Electronic Engineers (IEEE) Standard 802.11. Available at: http:Ngrouper.ieee.org/groups/802/1l/index.html.

(2) National Institute for Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications 140-l. Available at: http://www.itl.nist.gov/fipspubs/fipl40-1.htm.

(3) National Institute for Standards and Technology Federal Information Processing Standards Publications 140-2. Available at: http://www.itl.nist.gov/fipspubs/by-num.htm.

5. Explanation of abbreviations. Abbreviations used in this letter are explained in the glossary.

6. Responsibilities.

a. The command designated approval authority (DAA), appointed in accordance with (IAW) AR 380-19, is responsible for ensuring that all wireless local area networks (LAN) and PED technologies, as a minimum, adhere to the requirements outlined in this policy.

b. Currently fielded wireless LAN and PED technologies that are not in compliance with this policy must have migration plans developed to ensure the systems will meet the requirements of this policy. 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.

7. Requirements. Pilot and fielded wireless LANs and PEDs with LAN connectivity must meet the same certification and accreditation security requirements as wired LAN Automated Information Systems (AIS) per AR 380-19, AR 380-53, AR 25-1, and Department of Defense Instruction (DODI) 5200.40. Pilot projects must consider the following requirements during the development of the system:

a. Wireless solutions will be engineered to preclude backdoors into the Army's LANs. Backdoors could be caused by either unprotected transmissions or unprotected PEDs entering a network. Consideration of both factors must be evaluated in the design of a wireless solution.

b. 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.

c. Institute for Electrical and Electronic Engineers Publication 802.11, the industry standard for wireless LAN equipment, is the standard to consider when acquiring wireless LANs.

d. 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.

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

(1) ESSID 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.

(2) 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 an AIS.

f. For situations requiring protection of sensitive information, wireless LAN and PED solutions must fully implement a NIST FIPS 140-I or 140-2 level 1 validated crypto module using Triple Data Encryption Standard (3DES), or the new Advanced Encryption Standard (AES). Wireless LANs transmitting unclassified data that is not of a sensitive nature will require encryption using level 1 NIST FIPS 140-I or 140-2 validated crypto modules if they are connected to LANs that handle sensitive information. National Security Agency (NSA) approved type 1 encryption must be used for any situation requiring protection of classified information.

(1) Wired equivalent privacy (WEP) security protocol built into the IEEE 802.11 standards for wireless LANs does not use a FIPS-validated crypto module and has been found by the cryptographic community to have fundamental flaws. Those implementing wireless LANs must investigate additional security measures for data confidentiality and network intrusion protection, such as the use of Virtual Private Network (VPN) gateways that use FIPS-validated crypto modules.

(2) A more secure encryption for the 802.11 standards is currently being evaluated, but it is not known if a software/firmware upgrade to the more secure encryption will be possible or if the new encryption scheme will be FIPS-validated.

(3) Those planning wireless LAN solutions must consider that migration to more secure wireless LAN technologies could mean costly replacement of equipment.

g. 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, worms, and malicious code. The network infrastructure must accommodate anti-virus software updates for all desktops and servers that support PEDs.

h. 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.

i. PEDs with wireless communication capabilities will not be permitted inside a sensitive compartmented information facility (SCIF) 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 it's antenna has been removed/physically disabled. However, the agency in charge of any given SCIF is the authority for the procedures to move PEDs in or out of their facilities (See Joint DoDIIS/Cryptologic Sensitive Compartmented Information (SCI) Information Systems Security Standards, chap 15, and AR 380-19, para 2-13.) The various wireless and wired interconnection capabilities of PEDs present a significant risk that classified information will be compromised over an unclassified medium.

j. In no instance will a PED without strong identification and authentication (I&A) (that is, login and password) 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.

k. 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 nonrepudiation 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.

l. Personal Area Networks (PAN) (including Bluetooth) will not be utilized for transmitting sensitive information unless the data is encrypted with a FIPS-validated crypto module or the area in which the PAN devices communicate (within approximately 30 ft) is within a physically controlled and radio frequency-secured area.

m. 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 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 certificates and by allowing customers to run their own WAP gateways for secure, direct connections to web-based resources.

n. WAP gateways will be installed in the top level architecture (TLA) of Army installation networks so that wireless access to web-servers may be properly controlled and monitored by firewalls and intrusion detection systems (IDS).

o. 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.

p. 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. Submit spectrum supportability requests to the US Army C-E Services Office, 2461 Eisenhower Avenue, Suite 1200, Alexandria, VA 22331-2200.

q. All users being issued a PED must be provided security awareness training regarding the physical and information security vulnerabilities of the device.

r. Army commands and activities whose members use PEDs that synchronize with desktop computers on Army networks will adopt the following security measures and write them into command AIS security policies, security awareness and training, and network user agreements:

(1) Only use applications that are approved by the local DAA.

(2) PEDs will only be connected to unclassified computers.

(3) Passwords, combinations, personal identification numbers (PIN) and classified information will not be stored on PEDs.

(4) Do not use a PEDs remote connectivity features while it is physically connected to a desktop personal computer (PC), particularly a networked PC, or otherwise connected to the network.

8. Considerations before acquiring and using wireless LANs and PEDs.

a. 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.

b. The following characteristics/limitations of wireless solutions must be considered prior to their use:

(1) Wireless solutions may create backdoors into Army LANs. 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.

(2) Wireless LANs are susceptible to interference, interception, and can be jammed.

(3) Currently, there are three major wireless telephone transmission-multiplexing techniques in use by commercial wireless service providers in the U.S.: Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communications (GSM). Each transmission standard is incompatible with the others. Equipment operating using one standard cannot communicate with equipment using a different standard.

Glossary

Section I
Abbreviations

3DES
Triple Data Encryption Standard

AES
Advanced Encryption Standard

AIS
Automated Information System

AR
Army regulation

CDMA
Code Division Multiple Access

COTS
commercial off-the-shelf

DAA
designated approval authority

DISC4
Director of Information Systems, Command, Control, Communications, and Computers

DITSCAP
Defense Information Technology Security Certification and Accreditation Process

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODIIS
Department of Defense Intelligence Information System

ESSID
Extended Service Set Identifier

FIPS
Federal Information Processing Standards

GSM
Global System for Mobile Communications

IEEE
Institute for Electrical and Electronic Engineers

I&A
Identification and Authentication

IAW
in accordance with

IDS
Intrusion Detection System

LAN
Local Area Network

MAC
Media Access Control

MCEB
Military Communications Electronics Board

NIST
National Institute for Standards and Technology

NSA
National Security Agency

PAN
Personal Area Network

PC
personal computer

PED
portable electronic device

PDA
personal digital assistant

PIN
personal identification number

PKI
Public Key Infrastructure

SCI
Sensitive Compartmented Information

SCIF
Sensitive Compartmented Information Facility

TDMA
Time Division Multiple Access

TLA
top level architecture

VPN
Virtual Private Network

WAP
Wireless Access Protocol

WEP
Wired Equivalent Privacy

Section II
Terms
This section contains no entries.

Section III
Special Abbreviations and Terms
This section contains no entries.

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

Distribution:

This publication is available in electronic media only and is intended for the following addresses:

HQDA (SASA)
HQDA (DACS-ZA)
HQDA (DACS-ZB)
HQDA (DACS-ZD)
HQDA (SAUS-OR)

HQDA (SACW)
HQDA (SAFM-AOA)
HQDA (SAILE)
HQDA (SAMR)
HQDA (SAALT)
HQDA (SAGC)
HQDA (SAAA-PP)
HQDA (SAIS-ZA)
HQDA (SAIG-ZA)
HQDA (SAAG-ZA)
HQDA (SALL)
HQDA (SAPA)
HQDA (SADBU)
HQDA (DAMI-ZA)
HQDA (DALO-ZA)
HQDA (DAMO-ZA)
HQDA (DAPE-ZA)
HQDA (DAEN-ZA)
HQDA (DASG-ZA)
HQDA (NGB-ZA)
HQDA (DAAR-ZA)
HQDA (DAJA-ZA)
HQDA (DACH-ZA)
HQDA (DAIM-ZA)
HQDA (JDIM-RM)

COMMANDING GENERAL
U. S. ARMY, EUROPE AND SEVENTH ARMY

COMMANDERS
EIGHTH U. S. ARMY
U. S. ARMY FORCES COMMAND
U. S. ARMY MATERIEL COMMAND
U. S. ARMY TRAINING AND DOCTRINE COMMAND
U. S. ARMY CORPS OF ENGINEERS
U. S. SPECIAL OPERATIONS COMMAND
U. S. ARMY PACIFIC
MILITARY TRAFFIC MANAGEMENT COMMAND
U. S. ARMY CRIMINAL INVESTIGATION COMMAND
U. S. ARMY MEDICAL COMMAND
U. S. ARMY INTELLIGENCE AND SECURITY COMMAND
U. S. ARMY MILITARY DISTRICT OF WASHINGTON
U. S. ARMY SOUTH

CF:
U. S. ARMY RECRUITING COMMAND
U. S. ARMY COMMUNITY AND FAMILY SUPPORT CENTER