ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION
INTEGRATION

JUN 0 2 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF COMBATANT COMMANDS
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG)

References: (a) Use of Commercial Wireless Devices, Services, and Technologies in the DoD GIG, DoD Directive (DoDD) 8100.2, April 14, 2004
(b) Global Information Grid (GIG) Overarching Policy, DoD Directive 8100.1, September 19, 2002
(c) Ports Protocols and Services Management, DoD Instruction 8551.1, August 13, 2004

This memorandum and attachment provides supplemental policy and guidance to DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD GIG (reference a). Its goal is to enhance overall security guidance and to create a foundation and roadmap for increased interoperability that embraces open standards regarding WLAN technologies.

This policy applies to WLAN (i.e., Institute of Electrical and Electronics Engineers 802.11) devices, systems, and technologies that have the capability to store, process, or transmit unclassified information but does not apply to other wireless or cellular technologies (i.e., 2.5G, 3G, 4G, 802.15.1 (Bluetooth), proprietary Radio Frequency, 802.16 (WIMAX), and Infrared), which are also addressed in reference (a).

WLAN devices, systems, and technologies must be acquired, configured, operated, and maintained to ensure joint interoperability, open standards, and open

architectures, per references (a) through (c). New acquisition of WLAN devices shall comply with the standards set forth in paragraph 1.c.(1) of Attachment 1 starting in FY 2007. Migration plans for the compliance of legacy WLAN systems must be submitted to the Director, Communications Directorate of ASD(NII)/DoD CIO within 180 days of this memorandum. Compliance with all other aspects will be presented annually to the DoD CIO, per paragraph 3.c.(3) of Attachment 1.

The ASD(NII)/DoD CIO POC for this policy is Mr. Danny Price, 703-607-0269 or danny.price@osd.mil.

John G. Grimes

Attachment:
As stated

Use of Commercial WLAN Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

Policy

1. Policy. The following are requirements for Wireless Local Area Network (WLAN) technology standards, product validations, and security standards.

a. Standards-based WLAN technologies. DoD components must ensure that only standards-based WLAN technologies are deployed. WLAN devices, systems, and technologies must comply with IEEE 802.11 body of standards.

b. WLAN product certifications and validations. DoD Components must ensure that WLAN products are certified and validated for secure end-to-end communications and interoperability. Any WLAN product with cryptographic functionality must be National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) 140-2 overall Level 1 validated (at a minimum). In addition, any Information Assurance (IA) enabled WLAN product must be National Information Assurance Partnership (NIAP) Common Criteria (CC) validated. Per the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), reference (d), components shall ensure that the system meets overall end-to-end security requirements as approved by the DAA. Per the Interoperability and Supportability of Information Technology and National Security Systems Directive, reference (e), components shall ensure that the system meets overall end-to-end interoperability requirements as approved by the Joint Interoperability Test Command (JITC).

When available, WLAN-enabled solutions must be validated under the NIAP CC as meeting applicable U.S. Government WLAN protection profiles (e.g., Portable Electronic Device (PED), client, or access system) for basic or medium robustness environments, as determined and approved by the Designated Approving Authority (DAA).

(1) WLAN product commercial interoperability certifications. WLAN-enabled devices (i.e., Network Interface Cards (NIC) and Access Points (AP)) that store, process, or transmit unclassified information must be Wireless Fidelity (Wi-Fi) Alliance certified (for 802.11a, b, or g interoperability) and Wi-Fi Protected Access 2 (WPA2) Enterprise certified (for 802.11i interoperability). Starting in FY 2007, all new acquisitions of WLAN-enabled devices must be Wi-Fi and WPA2 Enterprise certified, when available. Wi-Fi and WPA2 certifications do not preclude the requirements of DISA Joint Interoperability Test Command (JITC) policies, detailed in reference (e).

(2) Data-in-transit NIST FIPS validation. Per DoDD 8100.2 (reference (a)), encryption for unclassified data in transit via WLAN-enabled devices, systems, and technologies must be implemented end-to-end over an assured channel and be validated under the NIST Cryptographic Module Validation Program (CMVP) as meeting

requirements per FIPS 140-2 at a minimum Overall Level 1. If WLAN infrastructure devices which store keying information are used in public unprotected environments, then those products must meet FIPS 140-2 Overall Level 2. Starting in FY 2007, all new acquisitions of WLAN-enabled devices must comply with paragraph 1.b.(1) and meet FIPS 140-2 validation criteria.

(3) Data-at-rest NIST FIPS validation. Data-at-rest encryption shall be implemented using either individual files, the file system (e.g., directories or partitions), or whole disk encryption/memory card. In recognition of the increased risks via wireless points of entry and the mobile nature of PED, WLAN-enabled PEDs must use encryption that is validated as meeting FIPS 140-2 Overall Level 1 or Level 2 requirements, as dictated by the sensitivity of the data. All sensitive unclassified data must be encrypted.

(4) Personal firewall NIAP Common Criteria validation. WLAN-enabled PEDs must use personal firewalls. Personal firewalls must be NIAP CC validated as meeting U.S. Government protection profiles, when available, per references (f) and (g).

(5) Antivirus NIAP Common Criteria validation. WLAN-enabled PEDs must use antivirus software when data services are to be used on those devices. Antivirus software must be NIAP CC validated as meeting U.S. Government protection profiles, when available, per references (f) and (g).

(6) WLAN NIAP Common Criteria validation. WLAN access systems (i.e., access points, security gateways, or wireless switches), and WLAN Network Interface Cards (NICs) must be NIAP CC validated as meeting U.S. Government protection profiles, when available, per references (f) and (g).

c. WLAN security standards. DoD Components must ensure that WLAN-enabled devices, systems, and technologies use a robust defense-in-depth security approach that includes confidentiality, integrity, and availability mechanisms. DoD Components must ensure that standards-based authentication and encryption are used.

(1) WLAN authentication and encryption. Starting in FY 2007 for all new acquisitions, DoD Components must implement WLAN solutions that are IEEE 802.11i compliant and are WPA2 Enterprise certified, that implement 802.1X access control with EAP-TLS mutual authentication, and a configuration that ensures the exclusive use of FIPS 140-2 minimum overall Level 1 validated Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) communications. Migration plans for legacy WLAN systems that do not support a Wi-Fi Alliance WPA2 certified 802.11i implementation with a FIPS 140-2 validated cryptographic module must be reported to the DoD CIO within 180 days of this policy memorandum, per paragraph 3.c.(2).

(2) Strong identification and authentication. Per reference (a), WLAN devices, systems, and technologies must use strong identification and authentication (I&A) (i.e., two factor, at minimum) at the device and network levels in accordance with published DoD policies and procedures. When "something you have" is one of the authentication factors, the item in possession must be something other than the device providing network communications.

d. WLAN intrusion detection. DoD Components must ensure that network intrusion detection systems continuously monitor wireless activity and wireless related policy violations on DoD wired and wireless networks.

Per references (f) and (g), Wireless Intrusion Detection Systems (WIDS) must be validated under the NIAP Common Criteria, when available, as meeting applicable U.S. Government protection profiles for basic or medium robustness environments, as determined and approved by the DAA.

(1) Wireless intrusion detection system. WIDS are required for all DoD wired and wireless local area networks (LAN). WIDS monitoring will ensure full awareness of any wireless activity within DoD network environments.

(2) Continuous-scanning WIDS. WIDS must continuously scan for and detect authorized and unauthorized activities. Continuous scanning is 24 hours/day, 7 days/week.

(3) Location-sensing WIDS. WIDS must include a location-sensing protection scheme for authorized and unauthorized wireless devices. The WIDS location-sensing capability must provide information that enables designated personnel to take appropriate actions.

2. Exception to policy

a. WLAN Security Exceptions. In instances where WLAN devices, systems, or technologies are not used in accordance with this policy (especially per paragraph 1.c. (1)), DAAs must approve a documented justification for the use of non-compliant WLAN devices, systems, or technologies during the DITSCAP, per reference (d).

b. Type 1 Device Exceptions. Use of National Security Agency (NSA)-certified Type I devices are also acceptable for unclassified data when operating in the secure mode, but are not the preferred solution. Certain Type 1 WLAN devices are proprietary in nature and are not interoperable with 802.11i solutions. When non-interoperable Type I devices are used for unclassified networks, the DAA must include justification during the DITSCAP C&A.

3. Responsibilities

a. The Director of Communications Programs & Policy (OASD[NII]), shall monitor all DoD wireless activities and provide guidance on the structure and input of reports submitted to OASD (NII), per paragraphs 3.c.(2) and 3.c.(3).

b. The Director of National Security Agency shall develop medium and high assurance protection profiles for PEDs, personal firewall, antivirus, and WIDS by 2007.

c. The Heads of the DoD Components must:

(1) Ensure that all new WLAN procurements comply with this memorandum starting in FY 2007.

(2) Submit to the DoD CIO/OASD (NII) Wireless Directorate within 180 days of this policy memorandum, specific migration plans for the compliance of legacy WLAN systems.

(3) Military Services will submit reports that contain compliance status and issues/challenges related to the implementation of this policy to DoD CIO (specifically, OASD (NII) Wireless Directorate) 180 days after the signing of this memorandum and annually thereafter.

(4) Ensure that joint interoperability is promoted through the adoption of IEEE 802.11i standards-based, WPA2 Enterprise certified products with FIPS 140-2 validation. If a WPA2 Enterprise certified product with FIPS 140-2 validation is not selected, the DAA must document the analysis of alternatives and explain non-compliance during certification and accreditation to denote acceptance of a non-standard security solution and the potential impact that a loss of interoperability imposes on the system, DoD users, and the GIG.

(5) Prepare and execute incident response plans for WLAN intrusion detection events.

d. The Director, Defense Information Systems Agency must provide guidance for the development of incident response plans and standards for intrusion detection and prevention capabilities.

(1) In conjunction with JS/J6 will develop and provide system requirements and specifications for wireless solution interoperability and Net-readiness testing.

(2) Develop and provide specifications and systems engineering and integration guidelines for C2 capable Wireless Systems.

e. The Joint Interoperability Test Command (JITC) is the only DoD organization with the mandate and authority to certify that DoD Information Technology (IT) including National Security Systems (NSS) meet interoperability and net-readiness requirements for joint military operations, per references (e) and (h).). As part of this mandate, JITC is the responsible organization to conduct interoperability certification of wireless devices deployed within the DoD.

In the absence of Joint Staff validated requirements, such as pre-acquisition commercial product testing, JITC may perform interoperability testing and issue an Interoperability Assessment Memorandum. Once an interoperability assessment is conducted, these results may be used to issue an Interoperability Certification if the test criteria and configuration fit the later-approved Joint Staff requirements. JITC may also issue a DoD Standards Conformance Certification for wireless devices that implement standards that can possibly impact interoperability.

References

Reference: (d) DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40, December 30, 1997

(e) Interoperability and Supportability of Information Technology and National Security Systems, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01C, November 20, 2003

(f) National Information Assurance Acquisition Policy, NSTISSP No.11, June 2003

(g) Information Assurance (IA) Implementation, DoD Instruction 8500.2, February 6, 2003

(h) Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, DoD Directive (DoDD) 4630.5, November 12, 1992