DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 2075.1
DON CIO
30 Nov 2006

SECNAV INSTRUCTION 2075.1

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY USE OF COMMERCIAL WIRELESS LOCAL AREA NETWORK (WLAN) DEVICES, SERVICES, AND TECHNOLOGIES

Ref: (a) SECNAVINST 5239.3A of 20 Dec 04
(b) DODD 8100.2 of 14 Apr 04
(c) DODI 8500.2 of 6 Feb 03
(d) DODI 8500.1 of 24 Oct 02
(e) DODD 8100.1 of 19 Sep 02
(f) DODD 5200.40 of 30 Dec 97
(g) DODD 4650.1 of 8 Jun 04
(h) Federal Information Processing Standard (FIPS) Publication 140-2 of 25 May 01
(i) DODI 8520.2 of 1 Apr 04
(j) SECNAVINST 5000.2C of 19 Nov 04
(k) DODI 5000.2 of 12 May 03
(l) NSTISSP No. 11 of January 2000

Encl: (1) Definitions

1. Purpose

a. To provide guidance for application and use of commercial wireless local area network (WLAN) devices, services, and technologies. Specific to this instruction, and as defined in enclosure (1), the term WLAN refers to commercial standards-based WLAN devices, services, and technologies to encompass client connectivity, bridging, and remote access.

b. To specify authentication, encryption, certification and accreditation parameters to ensure security of the Department of the Navy (DON) WLAN environment.

c. To assign responsibilities within DON for the evaluation, registration and implementation of secure WLAN solutions.

d. To enhance the enterprise network capabilities of the

DON, including enterprise mobility within and between the office, garrison and deployed environments, consistent with references (a) through (l), through secure application of commercial standards-based WLAN devices, services and technologies.

2. Background

a. A governing principle of the Navy-Marine Corps information management (IM) and information technology (IT) team is to deploy joint, interoperable IM/IT solutions to enhance the Warfighter's overall effectiveness. In an age where network centric operations define our ability to integrate business and warfighting systems into a seamless interoperable environment, the line between the office, garrison and deployed environments is increasingly blurred, creating the need for flexibility and enterprise mobility.

b. Secure application of WLAN technology offers substantial opportunity to extend the ability to connect to the enterprise network and accomplish the Department of the Navy (DON) mission in a more flexible and mobile fashion. Wireless local area networks are core components of enterprise mobility. Strategically designed, they foster efficiency, agility and interoperability throughout enterprise network architectures.

c. Risk mitigation is always a consideration with the application of new technology. Loss of information or communications security, confidentiality or integrity, and the threat of denial of service (DoS) attacks represent risks typically associated with the WLAN environment. While malicious users may intentionally attempt to exploit vulnerabilities, lack of knowledge about WLAN standards and security practices can also lead to unintentional disruption, vulnerabilities and disclosure of sensitive information. Use of properly configured, commercially available, products greatly reduces these threats.

d. Typically, network security approaches for unclassified, wired networks assume that the wired, local area network (LAN) connection is essentially secure. Hence, security mechanisms focus on the Open System Interconnection (OSI) Layer 3 and above. While the physical medium of wireless networks have significant differences from that of wired networks, a number of technologies and approaches exist for securing networks and computer resources at Layer 3 and above. Many organizations attempt to utilize these technologies to secure the WLAN portion of their environment. However, this approach does not adequately mitigate risk specific to DON networks.

e. DON's approach to integrating commercial WLAN technology into the enterprise architecture is to secure the components of the network that directly pertain to the wireless portion of the WLAN to a level that is as, or more, secure than a wired local area connection. In general, this means focusing on securing the network at OSI Layer 2, i.e., the data link layer. With the exception of specific Layer 2 security measures on the wireless portion of the connection, the wireless client device will be maintained under the same specified configuration controls as applied to wired local area network devices for information assurance and security.

3. Definitions. Terms used in this instruction are defined in enclosure (1).

4. Applicability and Scope. This policy:

a. Applies to all DON personnel, contractors, and visitors that enter DON facilities or access DON IT unclassified systems and networks, including those owned, used, or operated on behalf of the DON.

b. Applies to all unclassified DON commercial WLAN devices, services, and technologies.

For any commercial WLAN device, service, or technology that operates in proximity to Information Systems (IS) and/or Sensitive Compartmented Information Facilities (SCIF) to which Director of Central Intelligence Directive (DCID) 6/9 and DCID 6/3 apply, other requirements beyond the scope of this policy may apply.

5. Policy

a. Precedence. This policy is consistent with Federal and

Department of Defense (DOD) policies related to the use of commercial WLAN technology, spectrum management, and information assurance. In case of conflict with other policies, requirements set forth by higher authority take precedence over the policy established in this instruction. Implementing organizations should identify any conflicting policies to the DON Chief Information Officer (CIO) for resolution.

b. Secure Deployment. WLAN solutions must be deployed securely. Careful consideration shall be given to wireless network design to avoid unintended interception and/or bypassing boundaries or perimeter protections. The appropriate Service specific or Secretariat Designated Approving Authority (DAA) must approve system designs and installations of WLAN technologies. References (a) through (i)

c. Authentication and Encryption. All WLAN traffic shall be protected, at a minimum, by a Federal Information Processing Standards (FIPS) 140-2 certified device that authenticates and encrypts at Layer 2 of the OSI model. Reference (h)

d. Additional Security Protection. The use of encryption at Layer 2 does not preclude the additional use of Layer 3 encryption to protect data over a wide area network (WAN), i.e., long-haul protection for connections to remote networks and services as needed. Reference (b)

e. Certification and Accreditation. New or existing WLAN devices, services, and technologies that are integrated or connected to DON networks constitute a change to the network and therefore must comply with references (c) and (d) respectively, and be certified and accredited in accordance with reference (f).

f. Frequency Management. DON components developing or acquiring spectrum-dependent devices or systems shall make a determination there is reasonable assurance of spectrum supportability consistent with reference (g). Efforts to obtain spectrum supportability, for spectrum-dependent devices or systems being developed, shall be initiated as early as possible during the technology development phase of the acquisition life cycle as per references (j) and (k).

g. Public Key Infrastructure (PKI). All implementations of

WLAN technologies within the DON must meet applicable DOD PKI requirements per reference (i). As technology advances, appropriate PKI-enabled wireless solutions shall be implemented.

h. Intrusion Detection Methodology. Include wireless intrusion detection methodologies for all wired and wireless systems. Actively screen on a regular basis for wireless devices to detect and prevent unauthorized access of DON IT systems (at DON or contractor premises). References (a) through (f)

6. Responsibilities

a. The Department of the Navy Chief Information Officer (DON CIO) shall:

(1) Provide strategic oversight and policy development for the secure application of commercial wireless technology throughout the DON.

(2) Ensure compliance with the commercial wireless technology requirements of reference (b) and related policies, procedures, standards and guidelines.

b. The DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall, subject to the authority of the DON CIO, implement and enforce guidance and procedures in accordance with this policy.

c. The Assistant for Administration, Office of the Under Secretary of the Navy (AAUSN), when functioning as DAA for Secretariat systems, shall:

(1) Ensure that WLAN security requirements specified in this policy are integrated into all systems under his cognizance.

(2) Control WLAN access to Information Systems under his cognizance to ensure that WLAN systems (including external interfaces to WLAN services) do not introduce vulnerabilities that undermine the assurance of the other interconnected systems.

(3) Conduct a thorough analysis based on compliance with the WLAN security requirements specified in this policy and only authorize operation of compliant systems under appropriate operational cognizance. References (b) and (f)

d. The Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RD&A)) shall:

(1) Consistent with this policy, integrate WLAN security provisions into acquisition management of all acquisitions containing WLAN technology. References (b) and (f)

(2) Monitor all new WLAN procurements for compliance with this policy.

(3) Mandate that all Program Executive Officers, Systems Commands and Direct Reporting Program Managers involved in acquiring (either developing or procuring) WLAN devices:

(a) Seek and conform to guidance from the Military Communications-Electronics Board (MCEB) concerning the use of WLAN systems. Reference (b)

(b) Comply with the evaluation and validation requirements for IA-enabled IT devices as per references (a), (l), and this policy.

e. The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) shall:

(1) Ensure that WLAN security requirements specified in this policy are integrated into all DON IT systems that use WLAN technology.

(2) Upon request, provide to the DON CIO via each Service's DON Deputy CIO, specific implementation timelines for legacy system compliance with this policy.

(3) Ensure that feedback of evaluations of WLAN technology be provided to the DON Wireless Working Group (DWWG) concerning strengths, weaknesses, vulnerabilities, mitigation techniques, and related security procedures.

(4) Ensure the appropriate Service-specific Designated Approving Authority:

(a) Integrates WLAN security requirements into all systems under appropriate cognizance per references (a) through (i).

(b) Controls WLAN access to Information Systems under appropriate cognizance to ensure that WLAN systems (including external interfaces to WLAN services) do not introduce vulnerabilities that undermine the assurance of the other interconnected systems per references (a) through (i).

(c) Conducts a thorough analysis based on compliance with the WLAN security requirements specified in this policy and only authorizes operation of those compliant systems under appropriate operational cognizance.

(d) Provides amplifying, Service-specific guidance with regard to wireless LAN implementations and the requirements for their accreditation and approval.

7. Effective Date. This instruction is effective immediately.

John J. Lussier
Department of the Navy
Chief Information Officer
(Acting)

Distribution:
Electronic only, via Navy Directives Website
http://neds.daps.dla.mil//

DEFINITIONS

Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Bridging. A device that connects two networks that may use the same or a different data link layer (Layer 2 of the OSI Model) protocol.

Commercial Wireless. Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands.

Department of the Navy Information Executive Committee (DON IEC). This is a corporate level board that advises the Department of the Navy Chief Information Officer (DON CIO) who in turn is the IM/IT advisor to the Secretary of the Navy (SECNAV). The committee is authorized to establish subordinate organizations and processes, as required, to effectively carry out their responsibilities. To better align technology and strategy, the committee established the DON Wireless Working Group (DWWG).

Department of the Navy (DON) Wireless Working Group for Enterprise Mobility. Chartered on December 9, 2005 by the Department of the Navy Information Executive Committee (DON IEC) to establish a governance framework and information repository to enable deployment of secure, interoperable, cost effective, and capability-enhancing wireless architectures. This group is designated to make recommendations to the DON IEC regarding wireless solutions and strategies suitable for enterprise application. It is referred to herein as the DON Wireless Working Group (DWWG).

Designated Approving Authority (DAA). The official authorized to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DOD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

Electromagnetic Compatibility (EMC). The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

External Interfaces. Interfaces, including commercial systems (such as a cellular/PCS or pager network not under control of the DAA), capable of carrying traffic between systems under control of the DAA (e.g., the DOD IS and a DOD wireless device).

Federal Information Processing Standards (FIPS). The standards issued by the National Institute of Standards and Technology for Federal computer systems (http:www.itl.nist.gov/fipspubs).

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in 40 U.S.C. 11103(a) (formerly section 5142 is the Clinger-Cohen Act of 1996).

Identification & Authentication (I&A). Process of accepting a claimed identity and establishing the validity of that claimed identity.

Information Assurance (IA). Measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information System (IS). The entire infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.

Local Area Network (LAN). A high-speed, fault-tolerant data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, and other devices.

Open System Interconnection (OSI). Developed by the International Standards Organization (ISO), the OSI model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The 7 Layers are described as follows:

a. Application (Layer 7) - This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.

b. Presentation (Layer 6) - This layer provides independence from differences in data representation (e.g. encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept.

c. Session (Layer 5) - This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

d. Transport (Layer 4) - This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

e. Network (Layer 3) - This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node.

f. Data Link (Layer 2) - At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer.

g. Physical (Layer 1) - This layer conveys the bit stream (electrical impulse, light or radio signal) through the network at the electrical and mechanical level.

Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to Personal Data Assistants, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, and hand-held/laptop computers.

Remote Access. The connection of a remote computing device to access distant network applications and information.

Secretariat Systems. Any Navy Headquarters level systems owned, operated or managed by those organizations directly reporting to the Secretary or Under Secretary of the Navy.

Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Spectrum Supportability. The assessment as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or a spectrum-dependent system during its expected life cycle is, or will be, available (that is, from system development, through development and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" is based upon, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation from Host Nations [Note 1], and consideration of Electromagnetic Compatibility (EMC).

[Note 1]: While an actual determination of spectrum supportability for a spectrum-dependent system within a particular country (i.e., Host Nation) may be possible based upon "spectrum supportability", the overall determination of whether a spectrum-dependent system has spectrum supportability is the responsibility of the Milestone Decision Authority (MDA) based upon the totality of spectrum supportability comments returned from those Host Nations whose comments were solicited.

Wide Area Network (WAN). A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently, wireless technologies use Infra Red, acoustic, Radio Frequency, and optical but, as technology evolves, wireless could include other methods of transmission.

Wireless Local Area Network (WLAN). A local area network that uses high-frequency radio waves rather than wires for communication between nodes. Throughout this document, the term WLAN refers to commercial standards-based WLAN devices, services, and technologies to encompass client connectivity, bridging, and remote access.