



**Headquarters Marine Corps**  
Command, Control,  
Communications, and Computers (C4)  
Information Assurance Division

---



**Marine Corps**  
**Information Assurance**  
**Enterprise Directive**  
*014 Wireless Local Area Networks*  
*(WLANs) V2.0*  
06 July 2007

FOR OFFICIAL USE ONLY

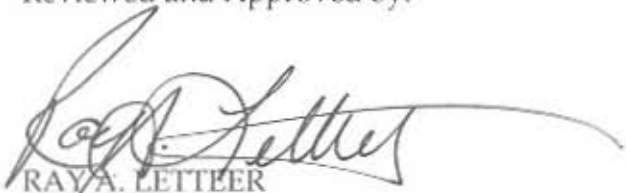
---

**FOREWARD**

The Director C4/ Marine Corps CIO and the Designated Accrediting Authority (DAA) issue Marine Corps Information Assurance Enterprise Directives (IAED). The IAED series provide modules that guide the implementation of policy direction established in MCO 5239.2. The modules provide procedural, technical, administrative, and supplemental guidance for all information systems, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the MCEN as well as other Marine Corps information systems. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing an element of the Marine Corps Information Assurance Program (MCIAP).

This module, "Wireless Local Area Networks (WLANs), Version 2.0," addresses security concerns, outlines minimal security configuration requirements, and establishes baseline access control guidelines for all WLANs connecting to the Marine Corps Enterprise Network (MCEN) or used in a production capacity at or on behalf of the Marine Corps.

Reviewed and Approved by:



RAY A. LETTEER  
MARINE CORPS DAA  
COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS  
INFORMATION ASSURANCE DIVISION



G. J. ALLEN  
BRIGADIER GENERAL, U.S. MARINE CORPS  
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS

**TABLE OF CONTENTS**

**SECTION 1.0 INTRODUCTION**..... 1

    1.1 Purpose..... 1

    1.2 Objectives ..... 1

    1.3 Scope ..... 2

    1.4 Action..... 4

    1.5 Cancellation ..... 6

    1.6 Distribution..... 6

    1.7 Recommendations..... 6

**SECTION 2.0 RESPONSIBILITIES**..... 7

    2.1 Designated Accrediting Authority (DAA)..... 7

    2.2 HQMC C4 IA and MCNOSC ..... 7

    2.3 Incident Response ..... 8

**SECTION 3.0 UNDERSTANDING WLANS** ..... 9

    3.1 Definition of a Wireless Local Area Network (WLAN) ..... 9

    3.2 Vulnerabilities Associated with Insecure WLANs ..... 9

**SECTION 4.0 WLAN STANDARDS** ..... 11

    4.1 Background..... 11

    4.2 Justification for Use..... 11

    4.3 Documentation Requirements ..... 12

    4.4 Restrictions on the use of Wireless Technologies..... 13

    4.5 Restrictions on the Purchase of Wireless Technologies..... 14

    4.6 Configuration Management Requirements ..... 14

    4.7 Configuration Requirements..... 14

    4.8 Testing Requirements..... 16

**SECTION 5.0 REFERENCES** ..... 18

**SECTION 6.0 ACRONYM LIST**..... 19

**SECTION 7.0 DEFINITIONS** ..... 21

## SECTION 1.0 INTRODUCTION

### 1.1 Purpose

Marine Corps Order (MCO) 5239.1 formally establishes the Marine Corps Information Assurance Program (MCIAP) and defines the responsibilities for protecting the Marine Corps information infrastructure as well as delineating Department of Defense (DoD) directives, instructions, and guidance governing DoD Information Assurance (IA). United States Marine Corps (USMC) IA Enterprise Directive 014 Wireless Local Area Networks (WLANs) outlines the security configuration and implementation standards for WLANs within the Marine Corps Enterprise Network (MCEN) boundary security framework.

### 1.2 Objectives

To ensure that the USMC:

**1.2.1** Protects the availability, authentication, confidentiality, integrity, and non-repudiation of both wired and wireless IT assets, including information transmitted using commercial WLAN wireless devices, services and technologies.

**1.2.2** Wireless IT assets do not adversely impact existing systems by causing electromagnetic interference (EMI) or other unintended electromagnetic consequences as determined by reference (j).

**1.2.3** Wireless technologies are afforded the safeguards required to protect USMC IT assets from the vulnerabilities associated with the use of commercial wireless local area networking technologies.

**1.2.4** Personnel using USMC information systems receive wireless security training commensurate with their duties and responsibilities.

**1.2.5** Wireless security-related technology research and development efforts are responsive to the requirements of the USMC.

**1.2.6** Encourages interoperability between Department of the Navy (DoN) enclaves and DoD agencies, as required.

### 1.3 Scope

This IAED applies to:

**1.3.1** Marine Corps components, organizations and personnel (government and non-government employees) that enter USMC facilities and/or access USMC IT systems. This includes any networks that process any USMC data whether stand alone, contractor provided, or directly connected to the MCEN backbone.

**1.3.2** All Marine Corps commercial wireless devices, services, networks and technologies intended for use in both ashore and afloat environments. Per Commandant of the Marine Corps (CMC) memorandum, Headquarters, Marine Corps (HQMC) Command, Control, Communications, and Computers (C4) is responsible for all networks and networked systems within the MCEN. The MCEN is defined as all garrison, tactical and NMCI networks that operate in accordance with paragraph 1.3.1. Therefore, Approval to Operate (ATO)/Approval to Connect (ATC) must be granted prior to installation of any commercial wireless technologies. Also includes, but is not limited to: commercial wireless data communication devices, networks, PEDs such as PDA's and personal computers, audio/video recording devices, scanning devices and any other technology capable of storing, processing or transmitting information via commercial-based technologies connected to any USMC internal networks, operated aboard USMC facilities or established in support of USMC personnel.

**1.3.3** The use of commercial wireless networking technologies in the USMC can be categorized into one of two "Zones". The security requirements of the network will depend on the "Zone" that your network corresponds to.

**1.3.3.1** Zone 1: Zone 1 is all wireless networks using commercial wireless technologies, that connect to the MCEN backbone, and/or stores, processes, or displays USMC operational data, processes any information that is sensitive in nature (HIPPA, Privacy Act, Financial, Personal, etc...) or any other information that may be considered DOD SBU.

**1.3.3.2** Zone 2: Zone 2 is all wireless networks using commercial wireless technologies, which do not fit into Zone 1, such as dedicated point-to-point RF connections secured by a FIPS 140 approved solution that operates at or above Layer 3 of the OSI model, or an infrastructure solution secured by the Harris SecNet 54 Type 1 solution (which operates at Layer 3 of the OSI model).

This IAED does **not** apply to:

**1.3.4** Receive-only pagers, Global Positioning Systems (GPS) receivers, hearing aids, pacemakers or other implanted medical or life support devices.

**1.3.5** Information systems used in Sensitive Compartmented Information Facility (SCIF) and Special Access programs to which references (f) and (g) apply.

**1.3.6** Bluetooth devices to include but not limited to, mice, keyboards, headsets, printers, and other peripheral devices. Because of the inherent vulnerabilities associated with the Bluetooth protocol, the use of Bluetooth devices is not authorized within the USMC. The DAA may, on a case-by-case basis, approve Bluetooth devices, but this is the exception, not the rule. The only current exceptions to this are DAA approved Bluetooth Common Access Card (CAC) readers. When properly configured these devices provide robust security as well as the ability to cryptographically sign and encrypt emails from wireless hand-held devices.

**1.3.7** Radio Frequency Identification (RFID). While not a true “networking” technology, RFID is fast becoming an essential part of the systems used for tracking and inventory of assets throughout DoD. While the use of this technology is advantageous when compared to traditional methods, there are inherent security concerns that must be addressed.

The two essential components of an RFID system are the tags (active, passive, and hybrid) and the readers. The tag is the identification device that contains information about the asset with which it is attached to. Passive tags are somewhat limited in the amount of data they contain, which severely limits the ability to encrypt the data resident on the tags. Active tags, on the other hand, have the ability to store much more information and they have the ability to provide more security for the information on the tags. The reader is the device that recognizes the tag and reads the information embedded on it. There is typically little or no security for the communication between the tag and the reader. Therefore, security must be implemented throughout the system. The firmware, edge/middleware, H/W devices, and the database that stores the relationship between the data on the tag and the item that it represents, must be properly secured. Since the use of RFID is essential in accomplishing certain missions and this is a relatively new and dynamic technology, the Marine Corps DAA will address each instance and determine acceptable risk on a case-by-case basis.

**1.3.8** Cellular wireless technologies. From a security perspective, cellular and cellular based data connections (wireless broadband) are as, or more, secure than a

typical Plain Old Telephone System (POTS) dial-up connection, Cable Modem, or DSL connection. Because of this, the use of cellular based wireless technologies are allowed as long as they are secured in accordance with the current Remote Access Service (RAS) policy, to include the use of an approved data encryption technology such as, IPsec VPN, SSL, TLS, SSH, or other DAA approved security solution.

**1.3.9 Harris SecNet 11 wireless device.** This device has been approved by the National Security Agency (NSA) for use on networks classified up to Secret. Because the security of the SecNet 11 device is based in the PCMCIA card and not in an external authenticating device/server, the SecNet 11 does not require independent DAA approval for its use. Once you have received permission from the local Spectrum Manager for its use and configured it in accordance with NSA policy/guidance, (from an IA perspective) it will be treated the same as any other local area network (LAN) device on your network.

Current policy does not support using a wireless client on any non-USMC approved wireless network to access a government/military network, example: accessing MCEN resources (including NMCI) from the neighborhood cybercafé (HotSpot) or from personal, (home/barracks) and hotel/airport wireless networks.

These standards are in strict conformance with applicable Federal laws and regulations, DoD directives and instructions, and other directive material contained in Section 5.0 of this document.

## **1.4 Action**

**1.4.1** This document is to be considered a "living document" as wireless networking technologies are in a near-constant state of change, this document will be reviewed on a semi-annual basis and updated as required.

**1.4.2** All USMC Commands shall implement this policy within their organizations.

**1.4.3** All operating activities shall budget for and execute the actions necessary to comply with this instruction.

**1.4.4** This instruction takes precedence over all previous USMC messages, instructions, and policies concerning commercial wireless networks. All wireless technology implementations in existence prior to this instruction must comply with this instruction immediately. Individual waivers will only be granted by the Marine Corps DAA for issues of safety, urgent combat operations or validated operational requirements. Failure to comply with this instruction will result in the termination of

Wireless LAN connectivity and the revocation of network accreditation. In addition, all commands requesting to operate a Wireless LAN(s) will be required to forward to the Marine Corps DAA an official Naval message with the following data:

**1.4.4.1** Command name, UIC, Location of network (Base, Building, Room)

**1.4.4.2** Current or proposed architecture, including: type of hardware, software, firmware and classification of data to be processed (submission of updated existing System Security Accreditation Agreement (SSAA) suffices for this requirement)

**1.4.4.3** Justification of wireless capability requirement

**1.4.4.4** Operational impact if not installed

**1.4.4.5** Prerequisite requirements (i.e., local Spectrum Manager approval, special administrator training, TEMPEST, HERO, HERF, RFI, etc.)

**1.4.4.6** Testing accomplished for approval/certification by appropriate technical agent (Marine Corps Network Operations and Security Command (MCNOSC))

**1.4.4.7** Schedule (to include length of time for temporary installations, and deployment date)

**1.4.4.8** Integrated logistics support requirements

**1.4.4.9** Training requirements

**1.4.4.10** Impact to existing systems if the request is approved or denied

**1.4.4.11** Risk assessment

**1.4.4.12** Contingency (Options/Fall-back should wireless operation fail)

**1.4.4.13** Documentation specifying the requirement for the use of the specific wireless networking technology in the request

**1.4.4.14** Interoperability Impact

**1.4.4.15** Point(s) of Contact with full name, rank, e-mail address(es) and phone number(s)



### **1.5 Cancellation**

None.

### **1.6 Distribution**

This document is approved for limited distribution. DoD components and other federal agencies may obtain copies of this manual through controlled Internet access only (limited to .mil and .gov users). Copies are located on the HQMC C4/IA web page <https://hqDoD.hqmc.usmc.mil/IA/Pages/Orders.asp>

### **1.7 Recommendations**

Recommendations for changes or amendments to these standards may be submitted in writing to the HQMC C4 IA Division. Recommendations will be evaluated and coordinated with the MCNOSC before taking the necessary action to change or amend this particular standard.

## SECTION 2.0 RESPONSIBILITIES

### 2.1 Designated Accrediting Authority (DAA)

Director, HQMC C4 appoints the Marine Corps DAA. In regards to this document, he/she is responsible for managing and overseeing WLAN operational standards and decisions on how they are managed within the MCEN.

### 2.2 HQMC C4 IA and MCNOSC

Per reference (a), HQMC C4 IA in conjunction with the MCNOSC, is tasked with providing centralized management and control of all MCEN WLANs. Specifically, it is responsible for:

**2.2.1** Implementing this wireless instruction across the MCEN.

**2.2.2** Developing and maintaining requirements for education, training, and awareness of wireless security issues in accordance with USMC IA requirements.

**2.2.3** Issuing wireless security standards to be used in the acquisition process for IT systems.

**2.2.4** Establishing and validating wireless security policies and coordinating IA requirements that cross service boundaries with Joint Staff.

**2.2.5** Actively participate in the DoD Knowledge Management (KM) process when evaluating wireless technologies.

**2.2.6** Ensuring that testing requirements are fulfilled, as applicable.

**2.2.7** Conducting periodic inspections to confirm compliance with all configuration requirements.

**2.2.8** Staying abreast of emerging commercial wireless technologies in order to properly develop/update current as well as future policies and procedures associated with the secure use of commercial wireless networking technology.

## **2.3 Incident Response**

**2.3.1** All security incidents involving wireless devices and/or technologies shall be reported IAW Ref (k) and (l).

**2.3.2** All security incidents involving wireless devices and/or technologies shall be reported immediately to MCNOSC via MARCERT and the MCNOSC Command Center, as applicable. This is in addition to enclave reporting procedures and any other reports that take higher precedence. This requirement includes all eight incident categories as defined by CJCSM 6510.01, Appendix B.

## SECTION 3.0 UNDERSTANDING WLANS

### 3.1 Definition of a Wireless Local Area Network (WLAN)

In a typical “wired” network, nodes communicate over a physical medium (Cat-3/5, Fiber, etc...). In a WLAN, nodes communicate over a radio frequency (RF) link. This can introduce numerous vulnerabilities to the wireless client as well as the enterprise network.

### 3.2 Vulnerabilities Associated with Insecure WLANs

**3.2.1** While wireless-networking technologies may offer many advantages over wired networks, if these devices are not properly secured, they introduce an unacceptable level of risk to the data transmitted over these wireless networks as well as the enterprise network that these devices are connected to.

**3.2.2** Wireless networks have all of the vulnerabilities typically associated with wired TCP/IP connections as well as the added vulnerabilities associated with the lack of physical protections afforded a wired connection. It is equivalent to installing an unlimited number of network hubs, in a three-mile radius outside a building that anyone can connect to. Additionally, wireless networking devices operate in a broadcast domain vice the switched network architecture normally associated with a wired network. Because of these inherent security risks, all commercial wireless networking devices are considered “external” connections and as such they must be approved by the Marine Corps DAA (via the MCNOSC Connection Approval Process (CAP)) prior to use. At no time will a command establish a commercial wireless network without first obtaining local spectrum manger and Marine Corps DAA approval.

**3.2.3** In addition to the vulnerabilities associated with the confidentiality, integrity, and availability of the data, deployed/tactical forces must also be aware of the potential vulnerabilities associated with the use of these non-Low Probability of Intercept (LPI)/Low Probability of Detection (LPD) devices. Although the typical maximum range of these WLAN networks is approximately 1000 feet (the range at which a commercial wireless card can successfully communicate with the associated access point), the actual detection range for these devices may exceed 30 miles in an open environment. These signals can be detected and isolated by using inexpensive commercial-off-the-shelf (COTS) equipment and freeware/shareware products. Additionally, deployed/tactical forces must also be aware of the potential denial of service (DoS) on wireless networks as well as the ability to locate forces using wireless technologies by direction finding (DF) the RF signal. Denial of service (DoS) attacks

may be intentional or unintentional as a result of interference from other friendly forces. As WLAN use increases, the potential for interference from friendly forces also increases. Currently the most widely used equipment operates under the 802.11b standard. Although channels 1-11 are specified for this standard in the US (12-13 in Europe and Canada, and 14 in Japan) only three of these channels can operate at one time without interference (1, 6, and 11). This limits the total number of separate co-located networks to no more than three in order to reduce interference. These devices operate on "unlicensed" frequencies. This means that the DoD has no control over these frequencies and must accept any interference from other devices operating in the same frequency range. For instance, the Harris SecNet 11 wireless cards operate in the same frequency range as 802.11b networks along with microwave ovens, baby monitors, cordless phones, Bluetooth devices and other commercial products. Additionally many foreign nations have restrictions on the use of these frequencies in their respective countries. These limitations may be addressed with the use of frequency changing equipment and reducing the power output of wireless devices. Local commanders must be aware of these vulnerabilities and take appropriate actions to mitigate these risks.

## SECTION 4.0 WLAN STANDARDS

The following section outlines procedures for requesting additional services. Future revisions will further define baseline standards for approved WLAN solutions. The WLAN standards are intended to ensure the, availability, confidentiality and integrity of data to, from, and for the MCEN and its authorized users. These standards may be updated periodically to ensure that newly discovered security vulnerabilities are addressed and mitigated in a timely manner.

### 4.1 Background

**4.1.1** Use of commercial-based wireless technologies provides USMC organizations the potential to improve portability and flexibility, increase productivity, and lower installation and operational costs.

**4.1.2** Risks are inherent in any networking technology to include wireless. The loss of information or communications security, confidentiality or integrity and the threat of denial of service (DoS) attacks represent risks typically associated with wireless communications. Malicious users may intentionally attempt to exploit vulnerabilities in wireless technologies in order to compromise the availability, confidentiality and integrity of USMC data, systems and networks. Lack of knowledge about wireless standards and security practices may also lead to unintentional disruption or vulnerabilities and disclosure of sensitive information.

**4.1.3** Appropriate management practices and Information Assurance policies regarding the secure use of wireless technologies are needed. USMC components must utilize the DoD Defense-in-Depth (DiD) Information Assurance (IA) strategy to mitigate information risks. This document integrates specific wireless security policies into the overall DiD IA strategy, as outlined in references (a) through (d).

### 4.2 Justification for Use

**4.2.1** The primary goal of this IAED is to use commercial wireless technologies to provide access to USMC data while maintaining the availability, confidentiality and integrity of the data as well as preventing unauthorized paths into the MCEN.

**4.2.2** The substitution of wireless for wired technology introduces numerous vulnerabilities into the network, which may be unacceptable or not cost effective to mitigate. Convenience and/or minor cost savings shall not be the sole justification for the use of wireless technologies.

**4.2.3** The Marine Corps DAA will approve each commercial wireless network installation on a case-by-case basis.

### **4.3 Documentation Requirements**

**4.3.1** Insecure wireless technologies that store, process, and/or transmit information may introduce vulnerabilities and risks to MCEN information systems and are highly susceptible to compromise or attack. Thus, USMC organizations shall comply with references (a) through (d) and be certified and accredited in accordance with reference (e).

**4.3.2** The addition of commercial wireless technologies to an existing approved network configuration boundary is considered a major configuration change and requires reaccreditation of the network, as a whole, IAW Ref (e). Temporary proof-of-concept wireless extensions to existing accredited networks may be documented via an addendum to the existing accreditation but will still require the Marine Corps DAA's approval prior to operation.

**4.3.3** Commercial wireless devices, services or technologies shall not be connected to MCEN operational systems or networks without prior approval of the local spectrum manager and the Marine Corps DAA. Only wireless systems that meet the criteria of this instruction or have been granted a waiver by the Marine Corps DAA, as well as having been accredited IAW Ref (e), may be approved for connectivity to the MCEN.

**4.3.4** The configuration of all wireless devices, including Personal Electronic Devices (PEDs), Personal Digital Assistants (PDAs) and Access Points will be controlled, managed, and well documented, IAW Ref (e). Periodic checks will be performed by the responsible command to confirm compliance with all configuration requirements.

**4.3.5** All commercial wireless components (Access Points/Base Stations/Clients/etc.) connected to the MCEN must be registered and approved by the Marine Corps DAA. These implementations will be subject to periodic penetration tests and audits.

**4.3.6** Prior to authorizing any connection of commercial wireless networks or devices, the Marine Corps DAA shall review proposed risk mitigation strategies such as passwords, virus protection, mobile code restrictions, intrusion detection, encryption and other preventive measures. The Marine Corps DAA will also assess the level of risk that the introduction of wireless technologies could unintentionally impact or

otherwise affect existing systems, networks, operations or security postures. This requires a formal security review in accordance with reference (c).

**4.3.7** USMC components shall use the DoD KM process in order to increase the sharing of wireless expertise and awareness across the DoN and DoD. All USMC components shall develop procedures to ensure participation in the KM process by contributing to vulnerability assessments, best practices and standard procedures for wireless device configuration. The Marine Corps DAA shall use the KM process to determine acceptable uses of wireless devices, services and technologies and to develop appropriate risk mitigation techniques.

**4.3.8** Prior to implementation of any wireless technologies, a site wireless survey and risk assessment must be performed to determine the condition of the environment in which the wireless technologies will be used. Points of note are other existing wireless networks, sources of interference, geographic location, physical protections, whether the wireless network reaches beyond those physical boundaries/protections, what organizations have personnel located within the proposed broadcast space, etc.

**4.3.9** Each site will have its own unique, site-specific conditions that must be included in the risk assessment. Examples of the data to be documented includes: type of data to be transmitted, denial of service vectors, types of wireless devices to be deployed (client, server, etc.), physical protections (e.g., remote field offices in commercial spaces), on-site/off-site networking staff, end users, acceptable use policy, etc. This site survey/risk assessment must be included in the accreditation package submitted to the MCNOSC C&A Section. Failure to provide this information will result in denial of the request.

#### **4.4 Restrictions on the use of Wireless Technologies**

**4.4.1** Wireless technologies used for storing, processing, and/or transmitting unclassified information shall not be used in areas where CLASSIFIED information is discussed, stored, processed, or transmitted without the express written consent of the Marine Corps DAA and the Service Certified TEMPEST Technical Authority (CTTA).

**4.4.2** The Service CTTA must evaluate the environment and equipment to be employed and must determine the appropriate minimum separation distance and countermeasures.



#### **4.5 Restrictions on the Purchase of Wireless Technologies**

**4.5.1** As per reference (m), Government Purchase Cardholders may not use the Government-wide Commercial Purchase Card to purchase any radio frequency (RF) devices except as noted in reference (m).

**4.5.2** It should also be noted that, IAW Ref. (m), splitting purchase requirements to avoid the simplified acquisition threshold is prohibited; constitutes fraud against the Government; and may violate provisions of the Service Contract Act (SCA) or the Davis Bacon Act.

#### **4.6 Configuration Management Requirements**

**4.6.1** All USMC commands will control and protect specific wireless configurations and information concerning same from unauthorized access, compromise, tampering, or exploitation.

**4.6.2** Configuration modifications and/or non-standard designs whose purpose is to extend the usable range or capabilities beyond those initially approved are prohibited without a waiver from the Marine Corps DAA.

**4.6.3** All non-type 1 encrypted DoN wireless networks shall be operated in "Infrastructure Mode" only. The use of "Adhoc" or "Mesh" configurations are prohibited.

#### **4.7 Configuration Requirements**

Measures shall be taken to mitigate risk of attack at the network, access point and client levels. These measures shall address not only threats from the outside but potential interference from friendly sources.

**4.7.1** The ESSID for a particular network will be chosen to reveal as little information as possible and the "broadcast SSID" feature of the access point will be enabled. Examples include choosing an ESSID that does not contain any identifying information about the organization, such as the command name, division title, unit designation, common phrases associated with the Marine Corps (i.e. Semper Fi, Devil Dog, etc.), personnel name, or product identifier. Default ESSIDs for wireless hardware will not be used on USMC networks. Additionally, all management settings on the access point to include user name and password must adhere to DOD standards.

**4.7.2** Careful consideration shall be given to network design to avoid bypassing boundaries or perimeter protections. Wireless solutions could create backdoors into USMC networks, a situation to be avoided. If a device receives information via a wireless technology and that device allows information to be placed directly into the USMC networks at the workstation level, then all boundaries or perimeters and host-based security devices have been bypassed. An example of this is client computers with wireless cards installed and active. By default many operating systems (to include Windows and OS X) will attempt to connect to any access point previously used. If the user does not disable this feature or delete these network configurations from their client computer, the client will continually try to connect to every wireless network currently defined on their system. This introduces vulnerabilities not only to the client but any network that the client connects to via a wired connection as well. An adversary can detect the client attempting to connect to a wireless network and spoof that network causing the client to connect to the adversary's wireless network while still connected to the wired network. Since this attack is against the client computer, it exists even if the command does not have any wireless networks installed. Because of this, all commands shall actively monitor for these client devices and provide training to personnel on ways to disable this feature. NSA has a very good guide for this and it is available at [www.nsa.gov/snac/support/I33-007R-2005.pdf](http://www.nsa.gov/snac/support/I33-007R-2005.pdf).

**4.7.3** Deficiencies in the 802.11 standard present specific vulnerabilities to the availability, confidentiality and integrity of all wireless traffic. At Layers 1 and 2 (of the OSI model), wireless technologies are susceptible to various DoS attacks. Other vulnerabilities in the standard allow for exploiting layers 3 through 7 via attacks on Layer 2, such as man-in-the-middle attacks and other ARP-based attacks. Because of these shortcomings, all "Zone 1" wireless network traffic between the mobile client and the access point will be protected, at a minimum, by a Federal Information Processing Standard (FIPS) 140-2 certified overlay solution (IAW Refs. h and i), that authenticates and encrypts at Layer 2 (OSI model).

**4.7.3.1** Due to the rapid growth in commercial WLAN technology, security concerns with 802.11i based solutions, and the associated time lag to get commercial WLAN hardware devices FIPS certified, the USMC mandates the use of "overlay" security solutions. These solutions secure the RF transmissions with a FIPS 140-2 approved overlay technology, which authenticates and encrypts at Layer 2 of the OSI model. This model protects the RF data in transit regardless of the commercial WLAN hardware used. By using this type of technology, we can ensure adequate security for these devices while allowing the operational forces the ability to use the latest commercial WLAN products available. All commercial wireless networks shall be approved by the local spectrum manager, as well as the Marine Corps DAA through the MCNOSC C&A process.

**4.7.3.2** Zone 2 wireless networks must be secured, at a minimum by a WPA-PSK or WPA-RADIUS solution. For a WPA-PSK solution the minimum pass-phrase length of 25 characters consisting of upper and lower case alphanumeric and special characters is required. For a WPA-RADIUS solution, the usernames and passwords must conform to DOD standards. Additionally, the access point must be configured in accordance with the guidance specified in 4.7.1. The Marine Corps DAA through the MCNOSC Connection Approval Process (CAP) must still approve these wireless networks.

**4.7.3.3** The use of encryption at Layer 2 does not preclude the additional use of Layer 3 encryption to provide "long-haul" protection for connections to remote networks/services. Layer 2 encryption protects the confidentiality of traffic between two devices on the same "local area network." Layer 3 encryption protects the confidentiality of traffic between two (possibly remote) IP addresses.

**4.7.3.4** Integrity checking (cryptographic signing) of traffic at Layer 2 can be used to mitigate the risk of disassociation attacks, de-authentication attacks, and other DoS session hijacking and man-in-the-middle attacks.

**4.7.3.5** Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are not FIPS 140 compliant and are insufficient for use in protecting USMC wireless assets.

## **4.8 Testing Requirements**

**4.8.1** USMC components shall perform periodic active searches/audits for wireless devices, services or technologies. Active electromagnetic sensing at USMC or contractor premises shall be conducted randomly (and at least quarterly) to audit the network and detect/prevent unauthorized access of DoD information systems. Audit logs will be maintained by the component conducting the assessment. USMC Information Assurance Personnel can request training to conduct such searches/audits through HQMC C4 IA Division.

**4.8.2** In environments where overall physical security is considered to be at a minimum (e.g., assets not located onboard a military installation) or where the 802.11 signal is detectable from a public area, these checks/audits will be performed on a weekly basis or immediately after a security incident.

**4.8.3** In environments where overall physical security is considered to be at a level consistent with a U.S. military base and no 802.11 signal is detectable from a public area, these checks/audits will be performed on a quarterly basis or immediately after a security incident.

**4.8.4** The Marine Corps DAA or Defense Security Service office (for contractor locations) may periodically audit the network(s) and may conduct active penetration(s) or Red Teaming and/or other forms of testing without obtaining prior notice or permission from the local network owner. This testing can include, but is not limited to: On-Line Surveys (OLSs), physical and logical network audits to ensure compliance in accordance with existing policy and restrictions based on on-going accreditation agreement.

## SECTION 5.0 REFERENCES

- a) DODD 8100.1, Global Information Grid (GIG) Overarching Policy, 19SEP02
- b) DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG), 14APR04
- c) DODI 8500.1, Information Assurance (IA), 24OCT02
- d) DODI 8500.2, Information Assurance (IA) Implementation, 06FEB03
- e) DODD 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 30DEC97
- f) DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, 18NOV02
- g) DCID 6/3, Protecting Sensitive Compartmented Information with Information Systems, 05JUN99
- h) FIPS 140-1, Security Requirements for Cryptographic Modules, 11JAN94
- i) FIPS 140-2, Security Requirements for Cryptographic Modules, 25MAY01
- j) MIL-STD-464, DOD Interface Standard, Electromagnetic Environmental Effects Requirements for Systems, 19MAR97
- k) OPNAVISNT 2201.2
- l) CJCSM 6510.01
- m) EBUSOPSOFFINST 4200.1a, Department of Navy Policies and Procedures for the Operation and Management of the Government Commercial Purchase Card Program (2SEP03)

---

## SECTION 6.0 ACRONYM LIST

AP	Access Point
ATO	Approval To Operate
ATC	Approval to Connect
CSA	Cognizant Security Authority
CETA	Certified EMSEC Technical Authority
DAA	Designated Accrediting Authority
DCID	Director of Central Intelligence Directive
DiD	Defense-in-Depth
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DoN	Department of the Navy
DoS	Denial of Service
EMI	Electro-Magnetic Interference
EMSEC	Emission Security
ESSID	Extended Service Set Identifier
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
IA	Information Assurance
IATO	Interim Authority to Operate
IDS	Intrusion Detection System(s)
IEEE	Institute of Electrical and Electronic Engineers
IT	Information Technology
KM	Knowledge Management
MC	Marine Corps
MCEN	Marine Corps Enterprise Network
MCIAAT	Marine Corps Information Assurance Assessment Team
MCIAGT	Marine Corps Information Assurance Green Team
MCIART	Marine Corps Information Assurance Red Team
NCAP	NMCI Connection Approval Process
NMCI	Navy/Marine Corps Intranet
NSA	National Security Agency
PCS	Personal Communications System
PDA	Portable Digital Assistant
PED	Portable Electronic Device(s)
PKI	Public Key Infrastructure

PPL	Preferred Products List
SSID	Service Set Identifier
SWLAN	Secured WLAN
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WI-FI	Wireless Fidelity

## SECTION 7.0 DEFINITIONS

**Access Point** - A wireless device that is analogous to a bridge as it bridges communications between two different physical media. It is also analogous to a hub in that on the wireless side all traffic is readable by any client device. The AP is the point at which the wireless LAN meets the wired LAN. All wireless "clients" access the wired network through the access point. Tools are available that permit a wireless client device to act as an access point.

**Ad-hoc** - The term given to the type of wireless network configuration in which any node can "talk" directly to any other node without having to "associate" with an access point first. (AKA Peer-to-peer). Ad-hoc, as the name implies, enables one to quickly setup a small wireless workgroup.

**Associate** - The act of two wireless devices (whether client to access point or client to client) establishing a logical connection with each other. A wireless client must first associate with an access point before it can send traffic through the access point (AP) to the wired LAN. At any time, an AP may be associated with multiple wireless clients but a wireless client may be associated with only one AP. The term given to the process by which a mobile device authenticates to the Access Point to be able to use the wireless network. Note: Has nothing to do with user authentication.

**Assured Channel** - A network communication link that is protected by a security protocol providing authentication, confidentiality and data integrity, and employs US Government approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements of authentication, confidentiality and data integrity protection for an assured channel: the Secret Internet Protocol Router Network (SIPRNET); Internet Protocol Security (IPSec); Secure Sockets Layer (SSL) v3; Transport Layer Security (TLS); Secure Multipurpose Internet Mail Extension (S/MIME) and systems using NSA-approved high assurance guards with link encryption methodology.

**Authentication** - The act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Security measure designed to establish the validity of a transmission, message, and originator.

**Availability** - One of the primary goals of Information Assurance, assurance in the timely and reliable access to data services for authorized users.

**Broadcast space** - That physical area within which a signal from an access point or wireless client can be detected/sniffed. (See also session space.)



**Client** - Typically a Wireless Network Interface Card (WNIC).

**Commercial Wireless Networking Devices** - Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands. This IAED does not apply to NSA certified type-1 devices, which are not intended for commercial use.

**Confidentiality** - One of the primary goals of Information Assurance, refers to limiting information access and disclosure to the set of authorized users and to preventing unauthorized access or disclosure to unauthorized users.

**Designated Approving Authority (DAA)** - The official designated by the local authority, which has the power to decide on accepting the security safeguards prescribed for an information system. NETWARCOM is the NAVY DAA; Headquarters Marine Corps C4 IA is the Marine Corps DAA.

**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 systems security. (DoD Instruction 5200.40)

**End-to-End** - From the end user device up to the security border of a DoD network or between two user devices connected by a DoD / non-DoD network (to include the wireless infrastructure's air interface).

**Federal Information Processing Standards (FIPS)** - The National Institute of Standards and Technology (NIST) Federal Information Processing Standards validation program.

**Global Information Grid (GIG)** -

- (A) The globally interconnected, end-to-end set of information capabilities associated process, and personal 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 section 5142 of the Clinger-Cohen Act of 1996.
- (B) Includes any system, equipment, software, or service that meets one or more of the following criteria:

- (1) Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software and services.
- (2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services.
- (3) Processes data or information for use by other equipment, software and services.
- (4) Non-GiG IT - Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

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

**Infrastructure Mode** - Infrastructure mode is used to incorporate wireless clients into the existing wired LAN infrastructure. There are three modes of WLAN operations: infrastructure, mesh, and ad-hoc (a.k.a. peer-to-peer). Ad Hoc mode is not permitted on the MCEN or for the transport of USMC data.

**Integrity** - One of the primary goals of Information Assurance, refers to the assurance that data has not been altered, intentionally or unintentionally, in transmission.

**Marine Corps Enterprise Network (MCEN)** - The MCEN infrastructure is defined as all NMCI, legacy, tactical systems and networks in the Marine Corps whether interconnected or stand-alone. It is the Marine Corps component of the Department of the Navy FORCENet.

**Mesh** - The term given to the type of wireless network (currently in development) in which nodes are able to act as repeaters for one another. Uses OSPF or a similar protocol to determine "paths" through the "mesh".

**Non-repudiation** - Ensuring that the identity of a user is verified/verifiable and cannot later be denied. (Example: a sender cannot deny sending the information.)

**Personal Communication System (PCS)** - Personal Communication System (or services) refers to a range of bi-directional converged digital wireless services. Mostly commonly used in modern cell phones and provides such services as text messaging,

voice communications (normal telephone and virtual "walkie talkie"), and mobile Internet (IP-based services).

**Personal Digital Assistant (PDA)** - A generic term for a class of small easily carried electronic device used to store and retrieve information.

**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 PDA, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, tablet PCs and laptop computers.

**Public Key Infrastructure (PKI)** - That portion of the security management infrastructure dedicated to the management of encryption keys and certificates used by public key-based security services. A PKI is a credentials service; it associates user and entity identities with public keys. A well-run PKI is the foundation on which the trustworthiness of public key-based security mechanism rests.

**RADIUS Support for Extensible Authentication Protocol (EAP)** - One of the RADIUS protocol limitations is that it can only implement password-based authentication: the password is transmitted either in the hash form (using MD5 hashing algorithm) or in the form of the response to a challenge (CHAP-password). The EAP protocol gives RADIUS the ability to work with a variety of authentication schemes including Public Key, Kerberos and smart cards.

**Service Set Identifier (SSID)** - Also referred to as a network name because essentially it is a name that identifies a Basic Service Set (BSS) and defines that wireless network. Commonly used acronym, which can denote the Extended Service Set Identification (ESSID), used in Infrastructure mode, and/or the Basic Service Set Identification (BSSID), used in Ad-hoc mode.

**Session space** - That physical area in which two-way communications can be successfully conducted between an access point and a client, or two access points. (See also broadcast space.)

**Wired Equivalent Privacy (WEP) Protocol** - An encryption scheme built into the IEEE 802.11 standard that was intended to provide a level of confidentiality through the air that one gets with a wired connection. It uses the RC4 encryption algorithm and a static key of either 40 or 102 bits plus an initialization vector of 24 bits for a total key space of either 64 or 128 bits. The WEP protocol does not provide a sufficient level of security to protect information on DoD networks.

**Wireless** - Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use infrared (IR), acoustic, radio frequency (RF), and optical but, as technology evolves, wireless could include other methods of transmission.

**Wireless Local Area Network (WLAN)** - A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

**Wireless Clients** - A wireless client is a desktop, laptop, or handheld device with a wireless network card able to communicate with an AP. The Client needs to be configured (automatically or manually) to use the same SSID as the AP to which it is connecting.

**Wi-Fi** - Short for Wireless Fidelity. Meant to be used generically when referring of any type of IEEE 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Wi-Fi is an industry certification that ensures equipment from different manufacturers work together with reasonable certainty. The term is promulgated by the Wi-Fi Alliance. Any products tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers".

**Wi-Fi Protected Access (WPA)** - WPA is a standards-based, interoperable security technology for Wi-Fi networks. It provides data protection by using encryption as well as access controls and user authentication. WPA can be enabled in two versions - WPA-Personal and WPA-Enterprise. WPA-Personal protects unauthorized network access by utilizing a set-up password. WPA-Enterprise verifies network users through a server. While this is a dramatic improvement over WEP, it is still not sufficient for USMC networks.

**Wi-Fi Protected Access 2 (WPA2, 802.11i)** - Wi-Fi Protected Access 2 provides network administrators with a high level of assurance that only authorized users can access the network. Based on the ratified IEEE (Institute of Electrical and Electronics Engineers) 802.11i standard, WPA2 provides enhanced security by having the ability to implement the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant Advanced Encryption Standard (AES) encryption algorithm. WPA2 can be enabled in two versions - WPA2 - Personal and WPA2 - Enterprise.

