**DEPARTMENT OF THE NAVY**
**HEADQUARTERS UNITED STATES MARINE CORPS**
**2 NAVY ANNEX**
**WASHINGTON, DC 20380-1775**

IN REPLY REFER TO:
MCO 5239.1
C4
NOV 18 2002

MARINE CORPS ORDER 5239.1

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS INFORMATION ASSURANCE PROGRAM (MCIAP)

Ref: (a) DoD CIO Guidance and Policy Memorandum No.6-8510, Department of Defense (DoD) Global Information Grid (GIG) Information Assurance (IA), 16 Jun 00
(b) DoDD 5200.28, Security Requirements for Automated Information Systems (AIS's), 21 Mar 88
(c) SECNAVINST 5510.36, Department Of The Navy (DON) Information Security Program (ISP) Regulation, 17 Mar 99
(d) DoD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97
(e) SECNAVINST 5239.3, DON INFOSEC Program, 14 Jul 95, (CH-1) 17 Jan 97
(f) OMB Circular A-130, Management of Federal Information Resources, 30 Nov 2000

1. Situation. The United States Marine Corps (USMC) will continue applying information technology (IT) to support warfighting. Users of IT are increasing dependence on network IT-based Command & Control systems (C2S) to process and transfer daily administrative and operational information. Consequently, external and internal threats to these systems increase the likelihood that a successful attack may degrade or wholly disrupt daily administrative and operational tasks. Therefore, it is incumbent upon every Marine to be an active member of the MCIAP. This MCO formally establishes the MCIAP and defines the responsibilities for protecting our information infrastructure. This order augments Department of Defense (DoD) directives, instructions, and guidance governing information assurance (IA) and delineates the responsibilities for Marine Corps Commands and Directorates. Detailed IA actions will be published separately in IA publications.

2. Mission. Implement IA policy on all IT resources procured, developed, operated, maintained, or managed throughout the Marine Corps Total Force Structure (MCTFS).

3. Execution. Per references (a) through (f) the Marine Corps will adopt a "life cycle management" approach in applying uniform standards for the protection of USMC IT resources that produce, process, store, and transmit information. The Marine Corps will also assess threats, vulnerabilities, and their associated risks to identify appropriate countermeasures to effectively reduce risks to an acceptable

operational level. System developers/acquirers will ensure, through certification of technical features, that all information systems under their functional area, sponsorship, or direction are developed, acquired, and managed in accordance with the provisions of this order. Furthermore, commanders will identify all information systems within their purview and will be responsible for these systems' site certification and accreditation.

a. Commandant's Intent and Concept of Operations.

(1) Commandant's Intent for the MCIAP:

(a) Develop an IA capability that supports a robust infrastructure-wide defense in depth.

(b) Establish procedures for reviewing the effectiveness of IA programs and policies.

(c) Establish a comprehensive framework for security controls over information resources.

(d) Conduct periodic reviews of existing policies and procedures, and update or modify as warranted by environmental and systemic needs.

(e) Assimilate new technologies and information processing methodologies in a flexible, pro-active program.

(f) Use web technology to the greatest extent possible in support of training and data gathering.

(g) Deliver annual IA awareness training, which covers individual responsibilities, and procedures to all users of Marine Corps IA resources. In addition, those personnel assigned specific IA duties, e.g., Designated Approving Authority (DAA), System Administrator (SA), Information Systems Security Managers (ISSM), and Information Systems Security Officers (ISSO), will receive detailed training relative to their duties.

(h) Continue to improve efforts to monitor network and system activities, as well as detect, report on, and take countermeasures against unauthorized activities.

(i) Establish an integrated readiness review and compliance process.

(2) Concept of Operations. IA is an element of Information Operations (IO) that is employed to defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

b. Organizational Responsibilities

(1) Commandant of the Marine Corps (CMC). The CMC executes the coordination of the MCIAP through the appointment of:

(a) Director, Command, Control, Communications and Computers (C4)/Chief Information Officer of the Marine Corps as:

1 Oversight authority for all matters and programs regarding the MCIAP.

2 Component Commander for the Marine Forces Integrated Network Operations (COMMARFOR-INO) to retain purview for all USMC INO matters.

3 DAA for the Marine Corps Enterprise Network (MCEN).

(b) Commander, Marine Corps Systems Command (COMMARCORSYSCOM) as principal DAA for all systems or applications acquired or developed under that command and for all applications or systems for which they are the functional sponsor or advocate.

(c) Director of Intelligence as principal DAA for all Special Access and Sensitive Compartmented Information (SCI) programs, including the physical facilities of the programs.

(d) Functional sponsors as the DAA for systems within their purview.

(2) Director, C4. The Director, C4 is responsible directly to CMC for IA policies and programs enacted throughout the Marine Corps. The Director, C4 will:

(a) Ensure Marine Corps representation to DoD, Joint and DoN IA Panels and working groups.

(b) Designate a Marine Corps Senior IA Officer responsible for the overall creation, promulgation, and execution of the MCIAP; development and maintenance of policies necessary to implement the MCIAP; standardization of USMC policies, procedures, and guidance to adhere to applicable National, DoD, and DoN IA Directives; and ensure Marine Corps IA requirements are validated, endorsed, and forwarded for inclusion in the DoN IA Master Plan.

(c) Coordinate with Commanding General, Training and Education Command (CG TECOM), to ensure IA training requirements are provided to all military members, civilian personnel, and contractors who have access to any portion of the DoD GIG information systems.

(d) Coordinate with COMMARCORSYSCOM and Commanding General, Marine Corps Combat Development Command (CG MCCDC) to

validate and endorse the Marine Corps communications security (COMSEC) procurement requirements during the development of the Department of the Navy Program Objective Memorandum (POM).

(3) CG MCCDC. In support of the IA program CG MCCDC will:

(a) Validate Marine Corps IA operational requirements to CMC (C4).

(b) Ensure IA requirements are incorporated into all systems' requirements development/determination documentation even if the IT is only a sub-component of the entire system.

(c) Ensure IA is incorporated into Marine Corps systems architecture that contains an IT component or discrete IT systems in order to meet current DoD, DoN, and Marine Corps IA specifications.

(d) Coordinate with the Director, Marine Corps Information Technology and Network Operation Center (MITNOC) the integration of enterprise level system interoperability.

(4) CG TECOM. In support of the IA program, CG TECOM will:

(a) Develop appropriate Military Occupational Specialty (MOS) Individual Training Standards (ITS) that include validated MCIAP requirements.

(b) Incorporate IA training and education into all pertinent Marine Corps training and appropriate formal schools to meet validated MCIAP requirements.

(c) Develop Marine Corps formal school IA training and education that encompasses validated MCIAP requirements.

(5) COMMARCORSYSCOM. In support of the MCIAP, COMMARCORSYSCOM will:

(a) Serve as technical lead for MCIAP execution for applications and systems developed or fielded by MARCORSYSCOM.

(b) Prepare and maintain the Marine Corps IA Equipment Master Plan, as requested by CMC (C4) in coordination with MCCDC, Space and Naval Warfare Systems Command (SPAWARSYSCOM), and the Director, MITNOC. Execute Marine Corps fielding, implementation, and operations of IA programs as defined in the plan.

(c) Budget for, procure, and field validated systems and products in support of Marine Corps IA requirements.

(d) Submit Marine Corps COMSEC POM requirements to support IA programs to CMC (C4) via MCCDC for validation and endorsement.

(e) Ensure Program Managers have IA requirements integrated at each milestone in the development of acquired systems that have an IT component or are discrete IT systems.

(f) Ensure that certification documentation is delivered to Marine Corps customers to support accreditation requirements of the DITSCAP, reference (d).

(g) Assign a Certification Agent for each information system developed and acquired under the sponsorship of MARCORSYSCOM.

(h) Establish and maintain a master file of accredited systems currently being used within the Marine Corps. Ensure supporting certification and accreditation (C&A) documents are analyzed for lessons learned, identification of system deficiencies for the duration of the system's life cycle. Incorporate these into process improvements and the Marine Corps IA Master Plan annually.

(i) Provide life cycle management support for IA products and systems.

(6) COMMARFOR-INO. The COMMARFOR-INO is responsible as the focal point in the defense of computer networks and systems. In support of the IA program COMMARFOR-INO will:

(a) Coordinate the defense of Marine Corps computer networks and systems as directed by the Commander, Joint Task Force for Computer Network Defense (JTF-CNO).

(b) Monitor Marine Corps Information Assurance Vulnerability Alert (IAVA) compliance and act as the Marine Corps' reporting agent for IAVA, and clearing house for Information Assurance Vulnerability Bulletins (IAVB).

(c) Coordinate Information Operations Condition (INFOCON) in response to Computer Network Attack and report the Marine INFOCON status to JTF-CNO.

(d) Coordinate, as required, with Combatant and Marine Force Commanders to provide network defense support for deployed units.

(7) Director, MITNOC. In support of the IA program Director, MITNOC will:

(a) Assume IA responsibilities for and control of the MCEN boundary level architecture. This architecture consists of connection points between the Marine Corps sites that comprise the MCEN and any external network, referred to as points of presence (POPs).

(b) Maintain and update certification and accreditation documentation of the MCEN in accordance with the DITSCAP. Ensure

supporting documents are analyzed for lessons learned, identification of system deficiencies, and for incorporation in process improvements and the Marine Corps IA Master Plan, annually.

(c) Conduct vulnerability assessments on the MCEN to maintain the highest level of security.

(d) Ensure Marine Corps websites are configured and maintained in compliance with prescribed National, DoD, and DoN policies and guidance.

(e) Ensure the Marine Intrusion Detection and Analysis Section (MIDAS) monitors network traffic between MCEN point of presence sites and the Defense Information Systems Network (DISN) for intrusions, incidents, and anomalies and provides appropriate impact assessment and response, in real time. Ensure the MIDAS provides a mechanism and guidance for local commands to monitor internal traffic for internal vulnerabilities, intrusions, incidents, and anomalies so they may provide appropriate impact assessment, response, and reporting in real time. Aggregate Intrusion Detection Systems (IDS) data and key network device logs and provide incident trend and correlation analysis of network traffic across the MCEN. Report major impacts on Marine Corps operations; violations of National, DOD, DoN and Marine Corps IA policies; and criminal acts conducted on Marine Corps IT resources through appropriate chain of command or law enforcement/counter intelligence agencies.

c. Command Responsibilities. Commanding Generals/Officers are responsible for the overall management of IA practices for all systems and networks within their purview. The C&A packages are required for IA systems and applications. C&A packages are required prior to operating on or connecting to the MCEN and must be submitted through the appropriate chain for approval. (These duties are normally delegated, but are not restricted, to the G-6/S-6 of the operational unit, base, post, or station.) The Commanding Generals/Officers shall:

(1) Appoint, in writing, an ISSM. Ensure the ISSM receives applicable training to carry out the duties of this function. The ISSM functions as the command focal point and principal advisor for IA matters on behalf of the Commanding Generals/Officers. The ISSM reports to the Commanding Generals/Officers and implements the overall IA program within his or her area of responsibility.

(2) Ensure an ISSO is designated as appropriate, for each information system and network in the organization and receives applicable training to carry out his or her duties. The ISSO acts on behalf of the ISSM to ensure compliance with IA procedures at the operational site or facility.

(3) Ensure all personnel performing IA functions, e.g., SAs and operators, receive initial basic and system specific training, as well as annual, refresher, and follow-on training.

(4) Provide IA awareness indoctrination and annual IA refresher training is conducted down to the user level and is tailored to specific site requirements.

(5) Ensure current IA standard operating procedures are available, used, and updated regularly for each information technology resource.

(6) Ensure computer intrusion incidents, or suspicion of any, are reported to MIDAS of the MITNOC.

(7) Review certification documentation for systems under their purview to evaluate and determine an acceptable level of risk, and accredit these systems accordingly.

d. User Responsibilities. An information system user is defined as any military, civilian, or contractor personnel who have authorized access to the DoD GIG or Marine Corps IT resources. The information system user has the following responsibilities:

(1) Comply with this MCO, directives, and guidance as established by higher headquarters.

(2) Receive indoctrination training, and attend annual IA refresher training.

4. Administration and Logistics. Recommendations for changes to this Order should be submitted to CMC (C4) via the appropriate chain of command.

5. Command and Signal

a. Signal. This order is effective immediately.

b. Command. This order is applicable to the United States Marine Corps to include Marine Corps Reserves and any personnel employed by or in support of MCTFS. Noncompliance of the policies set forth in this order may result in administrative or disciplinary action, to include non-judicial punishment or courts-martial.

J. R. THOMAS
Director, Command, Control,
Communications, and Computers

DISTRIBUTION: PCN 112345678