UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE, FMF
BOX 555300
CAMP PENDLETON, CALIFORNIA 92055-5300

REFER TO:
I MEFO 5239.1A
G-6/skw
25 Jun 02

I MARINE EXPEDITIONARY FORCE ORDER 5239.1A

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE, FMF INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) SECNAVINST 5239.3 of 14 Jul 95, Department of the Navy Information Systems Security (INFOSEC) (NOTAL)
(b) DoD 5220.22-M of January 95, National Industrial Security Program Operating Manual (NISPOM)
(c) Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0, October 29, 1999
(d) Department of the Navy Chief Information Officer Information Technology Standards Guidance (ITSG) (NOTAL)
(e) DoD 5200.40 of 30 Dec 97, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)
(f) NSTISSI No. 4012, of August 1997, National Training Standard for Designated Approving Authority (DAA) (NOTAL)
(g) OPNAVINST 2201.2 of 3 March 1998, Navy and Marine Corps Computer Network Incident Response
(h) Navy IA Publication 5239-01 Introduction to Information Systems Security
(i) Navy IA Publication 5239-04 Information Systems Security Manager's Handbook
(j) Navy IA Publication 5239-07 Information Systems Security Officer's Guidebook
(k) MCO 5271.1A IRM Standards and Guidelines Program
(l) IRM 5239.08A Computer Security Procedures
(m) SECNAV R 211930Z OCT 98 DoN World Wide Web Policy

Encl: (1) List of Acronyms

1. Situation. The United States Marine Corps will continue developing information technology (IT) to support war fighting. Users of these technologies are increasingly dependent on IT systems to process and transfer daily administrative and

operational information. Consequently, external or internal threats to these systems increase the likelihood that a successful attack may severely degrade or wholly disrupt the performance of daily administrative and operational tasks. Therefore, it is incumbent upon every Marine to be an active member of the I Marine Expeditionary Force (I MEF) Information Assurance (IA) Program (MEFIAP). This MEF Order will outline the MEFIAP and the responsibilities of those agencies tasked with protecting our critical processes that depend on information technologies. This Order implements Department of Defense (DoD) directives, instructions, and guidance governing IA and delineates the responsibilities for I MEF Commands and components. I MEF directives addressing detailed IA actions will be published separately.

2. Cancellation. I MEFO 5239.1

3. Mission. Establish responsibilities, policies and procedures for the I MEF Information Assurance Program implementing the provisions of reference (a).

4. Execution. Per references (a) through (m), the I MEF will adopt a “life cycle management” approach in applying uniform standards for the protection of I MEF information technology resources that produce, process, store, and/or transmit information. The I MEF will also assess threats, vulnerabilities, and risks to identify appropriate levels of certification and accreditation (C&A) for each information system developed by a program office and/or operated at a local site.

a. Commander’s Intent and Concept of Operations

(1) Commander's Intent for the MEFIAP

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

(b) Conduct periodic reviews and make quick, decisive changes to existing policies and procedures.

(c) Assimilate new technologies and information processing methodologies in a flexible, proactive program.

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

(e) Protect information and resources to the degree commensurate with their respective values.

(f) Employ efficient, cost-effective information-based security features on all information technology resources procured, operated, maintained, or managed by I MEF organizational components. An analysis of costs and benefits should be used to determine which procedures and security features are appropriate, including a realistic assessment of the remaining useful life of legacy systems compared with the cost of adding new security safeguards.

(g) Conduct an assessment of threats and identify the appropriate combination of safeguards from the IA disciplines.

(h) Apply an appropriate level of certification and accreditation for each specific information system developed by a program office and for each site employing networks and deployed information systems

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

(2) Concept of Operations

(a) 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) The security challenges confronting I MEF information and information systems are multiplying rapidly with the exponential growth of interconnected systems for producing and exchanging data and information. As interconnectivity increases and the threats to information and information systems become more sophisticated and diverse, I MEF systems become inherently more vulnerable to surreptitious access and malicious attack.

(c) The fast-paced advances of technology drive I MEF reliance on commercial technologies and services; however, many of these solutions may offer only minimal defense against IA threat activity and must be augmented by IA disciplines and focused management decisions to ensure protection of I MEF information and information systems.

(d) Information Assurance Properties and Services must be properly managed and protected as required by law, regulation or treaty. Facilitating the management and protection of resources requires the appropriate implementation of security measures providing the IA properties and services of:

1. Confidentiality. Supports the protection of both sensitive and classified information from unauthorized disclosure.

2. Integrity. Supports protection of information against unauthorized modification or destruction.

3. Availability. Supports timely, reliable access to data and information systems for authorized users, and precludes denial of service (DoS) or access.

4. Authentication. Supports verifying the identity of an individual or entity and the authority to access specific categories of information.

5. Non-repudiation. Provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

(e) Mission Criticality. Assessing the security requirements of any information system for the five IA properties requires a determination of the criticality of the information system to the organization’s mission, particularly the warfighter’s combat mission. Five categories of criticality are defined in reference (c), Administrative, Mission Support, and three categories classified as Mission Critical. Some information systems may have components that fit in more than one category. Mission criticality is one of the key determinants of information security requirements, the level of effort appropriate to the certification and accreditation of systems, and the technologies appropriate for implementing the required safeguards.

(f) Information Sensitivity. Information Assurance requirements also depend on the need to control disclosure. Disclosure may be restricted either because of national security classification levels (Confidential, Secret, and Top Secret), Special Access (Single Integrated Operations Plan – SIOP or Sensitive Compartmented Information – SCI) requirements, or for other sensitivity. Sensitive information is any information not specifically authorized as classified which the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest or the conduct of federal programs or the privacy of Department of Defense personnel.

b. Tasks and Responsibilities

(1) Organizational Responsibilities

(a) I MEF Command Element

1. Provide for the Designated Approving Authority for accreditation of I MEF information systems and networks.

2. Ensure full implementation and coordination of the I MEF Information Assurance Program.

3. Ensure the appointment in writing of the I MEF Information Systems Security Manager. The I MEF ISSM will serve as the senior ISSM for I MEF.

4. Ensure the appointment in writing of an Information System Security Officer, as appropriate, for each information system and network in the organization.

5. Direct the I MEF ISSM to ensure execution of responsibilities and duties outlined in reference (a).

6. Ensure the establishment of an I MEF INFOSEC Web Site and IA Help Desk.

7. Ensure the establishment of a Communications Information Systems and Networks (CISN) Training Working Group responsible for developing and coordinating IA training for all I MEF personnel. CISN members at a minimum will include the I MEF ISSM and Major Subordinate Command ISSMs.

8. Ensure the establishment of an I MEF Computer Emergency Response Team (IMEFCERT) responsible for maintaining, restoring, and preventing loss of service.

9. Ensure all personnel performing IA functions receive initial basic and system specific training, required certification, as well as annual recurring, refresher, or follow-on training.

(b) Major Subordinate Commands

1. Ensure full implementation and coordination of the I MEF Information Assurance Program.

2. Ensure the appointment in writing of an Information Assurance Officer to oversee and provide IA guidance to subordinate organizations.

3. Ensure the appointment in writing of an Information Systems Security Manager to oversee and implement the IA program within the command. This appointee may be, but need not be the same individual assigned as Information Assurance Officer. Where management and administrative functions have been consolidated within the MSC command element, the Commanding Officer may designate a single ISSM to manage IA for the entire command, and subordinate ISSMs need not be appointed.

4. Ensure the appointment in writing of an ISSO, as appropriate, for each information system and network in the organization. The ISSO will be responsible for implementing and maintaining the site's information system and network security requirements. For smaller commands, the same individual may perform ISSM and ISSO duties.

5. Provide oversight and management of the activity IA training program in accordance with all policies stated and referred to by this Order.

6. Ensure current standard operating procedures inclusive of IA practices and procedures, are available and used for all information technology resources.

7. Ensure IA awareness indoctrination, and annual IA refresher training is conducted down to the user level, tailored to specific site requirements.

(2) Individual Responsibilities

(a) Commanding General (CG), I MEF. The CG will serve as the Designated Approving Authority. The I MEF Assistant Chief-of-staff G-6 has been delegated the duties of the I MEF DAA. Further delegation of DAA authority is limited to officers of the grade of O-6 or above and civilians of grade GS-15 or equivalent except by prior coordination and authorization from CG I MEF.

(b) I MEF G-6. The I MEF Assistant Chief of Staff G-6 shall represent the CG I MEF as the DAA for all I MEF information systems. Specific guidance on DAA roles and responsibilities is available in reference (f). Whether fulfilling the duties as DAA for program or systems development or as a site DAA, the DAA shall:

1. Appoint, in writing, an I MEF Information Systems Security Manager. This role can be delegated to officers, government civilians of grade GS-12 or above, or contractors if specifically delineated in the contract.

2. Appoint, in writing, an I MEF Information Systems Security Officer for each Information System. The ISSO will be responsible for implementing and maintaining the site's information system and network security requirements.

3. Ensure the respective DITSCAP System Security Authorization Agreement (SSAA) delineates the applicable IA training requirements for users, operators, maintainers, administrators, and managers in accordance with this Order and all specified references.

4. Ensure those training requirements for specific roles (e.g., DAA, ISSM, and ISSO) are met prior to appointment.

5. Ensure the certification and accreditation, where applicable, of all I MEF information technology resources.

6. Provide CG I MEF representation to the Headquarters Marine Corps Information Assurance Program Management Office, subordinate working groups and other USMC-level working groups and study groups relating to IA.

7. Grant final approval to operate an Information System or network in a specified security mode.

8. Grant final approval to connect to I MEF Regional computer networks.

9. Oversee the IA Program for I MEF. Provide streamlined, simplified and standardized security guidance and policy.

10. Approve the classification level required for applications implemented in a network environment.

11. Ensure INFOSEC responsibilities are assigned to individuals reporting directly to the DAA.

12. Review the I MEF accreditation plan and sign the accreditation statement for the network and each Information System.

13. Allocate resources to achieve an acceptable level of security and to remedy security deficiencies.

14. Approve additional security services necessary to interconnect to external systems (e.g., encryption and non-repudiation).

15. Ensure sites and systems under the cognizance I MEF are accredited in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), reference (e).

16. Respond to Information Assurance requirements submitted by MSC Commanders.

17. Establish working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation. This may require a Memorandum of Agreement (MOA).

18. Develop and issue standards for critical IA components under CG I MEF cognizance. Examples of critical components are firewalls, virtual private networks (VPNs), and intrusion detection systems (IDSs)). Critical IA components ensure interoperability with I MEF, USMC, or other DoD systems and must be standardized and managed at a service level. Standards are documented in the DoN CIO Information Technology Standards Guidance, Chapter 3 reference (d).

19. Ensure full coordination of the MEFIAP execution with CG I MEF and Headquarters USMC.

20. Draft and maintain the I MEF IA Master Plan in coordination with reference (k). The IA Master Plan shall include identification and formal documentation of IA goals and objectives for I MEF, a strategy for achieving those goals and objectives, a description of IA programs, projects and initiatives that will result in the capabilities needed, and an IA risk management plan.

21. Advise program managers and the DAA in their responsibility to assign a capable Certification Agent responsible for completing the certification and accreditation process in accordance with the DITSCAP, reference (e).

22. Establish and maintain a master file of I MEF accredited systems. Ensure supporting certification and accreditation instructions are analyzed for lessons learned, identification of system deficiencies, and for incorporation in process improvements and the I MEF IA Master Plan.

23. Centrally acquire I MEF standard and specified IA products. Provide life cycle management support for centrally procured IA products and systems, to include operations and maintenance funding.

24. Establish and maintain an I MEF INFOSEC Web Site in accordance with reference (m), and an IA Help Desk as directed by CG I MEF.

a. I MEF INFOSEC Website. The I MEF INFOSEC Web Site shall provide access to IA Publications as well as other IA related references. It shall provide access to advisories, announcements, and a variety of resources on IA issues across I MEF and the USMC. The I MEF NIPRNET INFOSEC Web Site URL is http://158.238.50.42/g6/IA/IA.asp.

b. Information Assurance Help Desk. For routine technical and engineering assistance, an IA Help Desk will be established to support I MEF commands on IA matters and provides guidance on specific questions for securing and certifying systems.

25. Support the I MEF Computer Emergency Response Team by providing network analysis and management

tools to support the I MEF Computer Emergency Response Team mission.

26. Coordinate Defense Information Infrastructure (DII) connection approval with the Defense Information Systems Agency (DISA) for I MEF information systems and sites. Ensure sites with DII connections meet DISA accreditation requirements.

27. As required, provide Internet web hosting and demilitarized zone (DMZ) services for MSCs. A DMZ is a dedicated network segment that is used to separate public services from internal services.

28. Provide network operations, including monitoring and restoral functions.

29. Issue, publish and distribute guidance necessary to ensure National level (e.g., NSA) policies are followed and enforced.

(c) I MEF Information System Security Manager. The ISSM acts as the focal point and primary point of contact for all security matters pertaining to the Information Systems under the purview of the I MEF. The ISSM is responsible for ensuring that INFOSEC program requirements are met. The ISSM accomplishes this by performing, directing, coordinating, administering, and overseeing various activities and personnel. General guidance on ISSM roles and responsibilities is available in reference (i). The ISSM will be familiarized with reference (j) and shall:

1. Execute ISSM responsibilities outlined in reference (i), and develop the procedures and policies necessary to implement higher directives and regulations.

2. Review the accreditation documentation to confirm that any residual risk is within acceptable limits.

3. Review the accreditation documentation to ensure each Information System supports the security requirements as defined in the Information System and network security program. Verify that each Information System complies with the Information System security requirements, as reported by the Information Systems Security Officer.

4. Ensure any computer intrusion incident, or suspicion of one, is reported to MARCERT at https://www.noc.usmc.mil/Secure/MARCERT or DSN 278-5300.

5. Provide the I MEF DAA with monthly, quarterly, and annual summaries of reported I MEF computer incidents.

6. Develop the procedures and policies necessary to implement higher directives and regulations.

7. Provide timely advisories of newly identified vulnerabilities to subordinate ISSMs.

8. Provide high-level oversight and standardization for the system certification and accreditation process in accordance with reference (e) for all programs across I MEF.

9. Provide intrusion detection monitoring, on-line surveys, and activity analysis and assessment.

10. Ensure IA Vulnerability Assessments are conducted in support of the DITSCAP process for developing systems.

11. Ensure accredited sites and systems maintain the approved security posture throughout the life cycle of the system.

12. Develop and oversee I MEF IA training requirements and provide requirements to the I MEF Training Working Group (see item 3.B.(2)(c)6).

13. Ensure when classified or sensitive but unclassified information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as cryptography, and Protected Distribution Systems (PDS).

14. Provide systems and security engineering and integration testing and support for I MEF information systems and networks with IA requirements. Provide input, review, and recommended updates to IA Publications. Establish and execute capability to provide on-site assessments to I MEF MSCs, including vulnerability assessments.

15. Assist I MEF G-6 by gathering relevant threat information to assist in defining system security requirements.

16. Ensure infrastructure solutions incorporate appropriate IA safeguards.

17. Coordinate I MEF submission of reports on IA postures, to include training initiatives and overall progress in meeting IA goals and objectives.

18. Act as the High Assurance (Class 4) PKI coordinating authority for I MEF.

19. Provide initial basic and system specific training, required certification, as well as annual recurring, refresher, or follow-on training for all personnel performing IA functions.

20. Maintain the I MEF IA Publication Library as directed.

(d) Major Subordinate Command ISSMs. General guidance on ISSM roles and responsibilities is available in reference (i). The ISSM will be familiarized with reference (j) and shall:

1. Submit any IA Program Objective requirements to the I MEF ISSM to support IA programs as delineated in the I MEF IA Master Plan.

2. Execute the ISSM responsibilities outlined in reference (i).

3. Execute I MEF IA programs as defined in the I MEF IA Master Plan.

4. Conduct intrusion detection monitoring, and activity analysis and assessment.

5. Ensure any computer intrusion incident, or suspicion of one, is reported to the I MEF ISSM.

6. Assist I MEF ISSM by gathering relevant threat information to assist in defining system security requirements.

7. Request vulnerability assessment assistance when needed to validate IA controls and practices.

8. Conduct IA awareness indoctrination and annual IA refresher training down to the user level, tailored to specific site requirements.

9. Provide participation in I MEF Communications Information Systems and Networks (CISN) Training Working Groups.

10. Identify and establish computer security training requirements for military and government civilian personnel in accordance with reference (l).

11. Ensure development of I MEF required training plans for information systems.

(e) I MEF Information System Security Officer. The ISSO is responsible for implementing and maintaining security for an information system on behalf of the ISSM. The ISSO reports to the Command ISSM for INFOSEC matters and implements the overall INFOSEC program approved by the Designated Approving Authority (DAA). General guidance on ISSO roles and responsibilities is available in reference (j). The ISSO shall:

1. Ensure that the Information System is operated, used, maintained, and disposed of in accordance with Command security policies and practices.

2. Execute all ISSO responsibilities outlined in reference (j).

3. Enforce all security policies and safeguards on all personnel having access to the Information System.

4. Report the security status of the Information System to the ISSM, as required by the DAA.

5. Maintain a System Security Plan (SSP) per reference (e).

6. Ensure TEMPEST measures have not been altered.

7. Ensure that users and system support personnel have the required security clearances, authorizations, and the need-to-know to perform work on the Information System.

8. Ensure that all computers display the standard Department of Defense access-warning banner per Department of Defense Directive 5200.28.

9. Conduct user training and awareness activities under the direction of the ISSM.

10. Work with physical security personnel to ensure the physical protection of Information System assets.

11. Conduct security audits and ensure audit trails are reviewed periodically and that audit records are archived for future reference.

12. Create a security incident reporting mechanism for reporting incidents to the ISSM when the Information System is compromised.

13. Initiate protective or corrective measures if a security problem is discovered.

14. Conduct the Risk Assessment of the Information System using the methodology determined by the ISSM and approved by the DAA.

15. Ensure the Information System is accredited.

16. Assist the ISSM in Information System configuration management activities to ensure that implemented changes do not compromise the security of the system.

17. Provide technical contributions to the ISSM for the development of contingency plans for the Information System for which he or she is responsible.

(f) I MEF Computer Emergency Response Team

1. Defend all computer networks and systems within I MEF elements of the Defense Information Infrastructure through an aggressive risk management program.

2. When tasked, be responsible for the monitoring, restoral, and security of I MEF networks in accordance with reference (d).

3. Monitor the I MEF Information Assurance Vulnerability Alert (IAVA) compliance and act as the I MEF Reporting Agent for IAVA.

4. Coordinate and direct appropriate actions to ensure I MEF web pages resident on the World Wide Web are in compliance with prescribed Department of the Navy and Headquarters Marine Corps guidance.

5. Make Information Operations Condition (INFOCON) recommendations to the I MEF Command Center in response to a Computer Network Attack and report the I MEF INFOCON status

(g) Responsible Officers of Program of Record (POR) Systems. Responsible officers of I MEF POR systems will ensure Program Managers integrate information assurance requirements in the design of information systems, and that all systems are delivered to I MEF units with certification documentation to support accreditation requirements of reference (e).

(h) Commanding Officers and Officers-in-Charge. Provide overall management of IA at the unit level to:

1. Ensure all automated information systems or networks used by the command are individually and collectively accredited by the I MEF DAA or by the appropriate DAA in the case of information system services centrally procured or provided by another command.

2. Ensure that all of the requisite safeguards, as documented in the respective DITSCAP System Security Authorization Agreement (SSAA) are implemented and that the site maintains accreditation. Assess the need to reaccredit with each system configuration change. While it is expected that a certification agent, ISSM, or ISSO, will assist the commander in this effort, accreditation is considered a command responsibility.

(i) User Responsibilities. Information system users are defined as any military, civilian, or contractor personnel who have authorized access to Marine Corps information systems and the MCEN. The information system user has the following responsibilities:

1. Comply with this I MEF Order, directives and guidance as established by higher headquarters.

2. Attend indoctrination training, be certified (as appropriate), and attend annual IA refresher training.

5. Administration and Logistics

a. Administration. Recommendations for changes to this Order are invited and should be submitted to CG I MEF (Attn: G-6) via the appropriate chain of command.

b. Logistics. The Navy Staff Office IA Publication series provide specific guidance and direction on implementation of this Order. The IA publications detail specific roles and responsibilities and reflect the latest affordable, acceptable, and supportable procedures and products to ensure the security and protection of I MEF information. IA publication 5239-01, reference (h), introduces and summarizes the Department of the Navy's approach to IA. IA publication 5239-01 is intended to foster a common understanding of IA principles, concepts, and interrelationships among system planners, organizational managers, Information Systems Security Officers and Managers, and users. Appendix A to IA publication 5239-01 lists and describes the current and planned IA publications. The IA publications are maintained by Director, Communications Security (COMSEC) Material System (DCMS) and shall be updated routinely. The IA publications are available on the NIPRNET and the SIPRNET at the Navy INFOSEC Web Site.

6. Command and Signal

a. Signal. This Order is effective immediately.

b. Command

(1) This Order applies to all I MEF organizations and contractors that enter, process, store, or transmit unclassified, sensitive but unclassified (SBU) or classified National Security information using information systems or networks within I MEF. Additionally it applies to contractor operated or owned facilities under I MEF authority, which shall also comply with the guidelines of reference (b). This Order

encompasses all information systems and networks that are procured, modified, operated, maintained, or managed by I MEF organizational elements. If information in this Order conflicts with other issued policy, the more stringent policy applies. Enclosure (1) provides a list of acronyms used throughout this Order.

(2) All commands shall implement the guidance contained herein and all associated references. All developing and operating activities shall budget for, fund and execute the actions necessary to comply with this Order and the publications that support it.

//S//
P. P. MCNAMARA
Chief of Staff

DISTRIBUTION: List I/II

LIST OF ACRONYMS

C&A:	Certification and Accreditation
CMC	Commandant of the Marine Corps
COMSEC:	Communications Security
COR:	Central Office of Record
DAA:	Designated Approving Authority
DCMS:	Director, COMSEC Material System
DIA:	Defense Intelligence Agency
DII:	Defense Information Infrastructure
DITSCAP	Defense Information Technology Security C&A Program
DoD:	Department of Defense
DoN:	Department of the Navy
IA:	Information Assurance
IAAV:	Information Assurance and Assist Visit
INFOSEC:	Information Systems Security
IS:	Information System
ISSM:	Information Systems Security Manager
ISSO:	Information Systems Security Officer
NAVCIRT:	Naval Computer Incident Response Team
NIPRNET:	Sensitive but Unclassified Internet Protocol Router Network
NISPOM:	National Industrial Security Program Operating Manual
PKI:	Public Key Infrastructure
SBU:	Sensitive but Unclassified
SIPRNET:	Secret Internet Protocol Router Network
SSAA:	System Security Authorization Agreement
URL:	Uniform Resource Locator