



**UNITED STATES MARINE CORPS**  
MARINE AIR GROUND TASK FORCE TRAINING COMMAND  
MARINE CORPS AIR GROUND COMBAT CENTER  
BOX 788100  
TWENTYNINE PALMS, CALIFORNIA 92278-8100

5239.2A

6

JUL 15 2010

COMBAT CENTER ORDER 5239.2A

From: Commanding General  
To: Distribution List

Subj: THE MARINE AIR GROUND TASK FORCE TRAINING COMMAND (MAGTFTC), MARINE CORPS AIR GROUND COMBAT CENTER (MCAGCC) INFORMATION ASSURANCE PROGRAM (SHORT TITLE: MAGTFTC, MCAGCC IAP)

Ref: (a) DoDD 8500.1 Information Assurance (IA), 24 October 2002  
(b) DoDI 8500.2 IA Implementation, 6 February 2006  
(c) CJCSM 6510.01 Defense in Depth: Information Assurance and Computer Network Defense (CND), 24 June 2009  
(d) SECNAV M-5239.1 Department of the Navy Information Assurance Program, November 2005  
(e) MCO 5239.2  
(f) CJCSI 6510.01E Information Assurance and Computer Network Defense, 15 June 2004  
(g) DoDI 8570.01-M Information Assurance Workforce Improvement Program

1. Situation. MAGTFTC, MCAGCC 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 MAGTFTC, MCAGCC IAP. This Order formally establishes MAGTFTC, MCAGCC IAP and defines the responsibilities for protecting our information infrastructure. This Order augments references (a) through (f) and delineates the responsibilities for local units and organizations. Detailed IA actions are published separately in the MAGTFTC, MCAGCC IA standard operating procedure.

2. Cancellation. CCO 5239.2.

3. Mission. Implement IA policy on communications and information systems (CIS) and IT resources procured, developed, operated, maintained, or managed at MAGTFTC, MCAGCC.

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

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

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 (C&A).

a. Commander's Intent and Concept of Operations

(1) Commander's Intent.

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

(b) Establish procedures for reviewing the effectiveness of local IA program(s) 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) Deliver annual IA awareness training, which covers individual responsibilities, and procedures to all users of Marine Corps IT resources.

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

(h) Establish an information assurance governance board to conduct compliance readiness reviews.

(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, reaction, and recovery capabilities.

b. Command Responsibilities. Commanding Generals and 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 all IT systems and applications. C&A packages are required for all IT systems used for the conduct of Marine Corps business 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 General shall:

(1) Appoint, in writing, a Command Information Assurance Manager (IAM) and Command Information Assurance Officer (IAO). Ensure the Command IA staff receives applicable training to carry out the duties of their function. The Command IA staff functions as the command focal point and principal advisor for IA matters on behalf of the Commanding General.

(2) Ensure unit IA roles are identified and are designated as appropriate, for each information system and network in the organization and

receives applicable training to carry out his or her duties. The unit IA staff acts on behalf of the Command IAM to ensure compliance with IA procedures at the operational site or facility.

(3) Ensure all personnel performing IA functions, e.g., IAMS, IAOs, System Administrator (SAs) and operators, meet certification requirements, outlined in reference (g) as well as annual, refresher, and follow-on training.

(4) Provide IA awareness indoctrination and ensure 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 the Marine Corps Computer Emergency Response Team of the Marine Corps Network Operations Security Command.

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

c. User Responsibilities. An information system user is defined as any military, civilian, or contractor personnel who have authorized access to the DoD global information grid or any IT resource processing government information. The information system user has the following responsibilities:

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

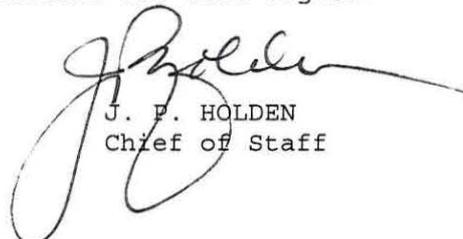
(2) Receive indoctrination training and complete annual IA refresher training.

5. Administration and Logistics. Distribution statement A directives issued by the Commanding General are distributed via e-mail upon request and can be viewed at: <http://www.29palms.usmc.mil/dirs/manpower/adj/ccotoc.asp>.

6. Command and Signal

a. Command. This Order is applicable to active-duty, reserve and civilian personnel aboard MCAGCC.

b. Signal. This Order is effective the date signed.



J. P. HOLDEN  
Chief of Staff