



UNITED STATES MARINE CORPS

MARINE FORCES RESERVE
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70146-5400

IN REPLY REFER TO:
5510
G-6

AUG 01 2011

FORCE POLICY LETTER 06-11

From: Commander, Marine Forces Reserve
To: Distribution List

Subj: INFORMATION PROTECTION PROGRAM (SHORT TITLE: IP PROGRAM)

Ref: (a) SECNAV M-5239.1
(b) CMC White Letter NO. 1-11
(c) Web Manager/Web Master Appointment Letter
(d) Social Media Manager Appointment Letter
(e) DoD Instruction 8570.01-M Information Assurance Workforce Program

1. Purpose

a. Per reference (a), this policy establishes the Marine Forces Reserve (MARFORRES) guidelines and procedures for the protection of information residing in the MARFORRES information environment. Appropriate, disciplined use of our communication and information assets is critical to properly protect our information and ensure success on the information and physical battlefields. Inappropriate use of government or personal computer and communication resources can have strategic consequences and threaten our national security. Accessing, transmitting, receiving, and sharing information through use of communication and Information Technology systems is a pivotal aspect of day-to-day operations throughout the Marine Corps. It is imperative that we adhere to regulations, take steps to mitigate vulnerabilities, and defend our networks and sensitive information from ongoing threats.

b. In an effort to reaffirm our commitment to Information Protection (IP) and strengthen our ability to operate successfully and securely in the Cyber Domain, we must ensure commanders at all levels are informed, vigilant, and aggressive in the protection of our information assets. Like other long-term campaigns, the Marine Corps is now entering an Information Protection Campaign in an effort to gain strategic advantages on the information battlefield. The plan to protect information must permeate from top-level leaders down to each individual that utilizes Marine Corps information, in any form. In accordance with reference (b), this document identifies specific tasks that must be accomplished to train personnel and protect information.

DISTRIBUTION STATEMENT D: All MARFORRES assets, approved for public release, distribution is unlimited.

Subj: INFORMATION PROTECTION PROGRAM (SHORT TITLE: IP PROGRAM)

2. Action

a. Assistant Chief of Staff, G-3/5

(1) Provide MARFORRES staff sections with education on operational security (OPSEC), as required.

(2) Ensure information on OPSEC is readily available to all members of MARFORRES on the Mission Assurance website.

b. The Force Family Readiness Officer (FRO)

(1) All FROs will complete the OPSEC Fundamentals Course, OPSE-1301, within 90 days of the date of this letter. The course is available at the Interagency OPSEC Support Staff website at www.iooss.gov.

(2) Future FROs will complete this training within 30 days of appointment.

c. Public Affairs Officer. The Public Affairs Officer will ensure that all Social Media Content Managers and Webmasters are designated in writing and will complete the OPSEC Fundamentals Course per references (c) and (d).

d. Information and Security Personnel

(1) Review and ensure the command's processes for authorizing access to classified information and submitting requests for investigation are based on established requirements and not convenience, and that all personnel who will handle classified information or will be assigned to sensitive duties are appropriately vetted. A review and report on both topics shall be done annually each July.

(2) Ensure all Marines, Civilians and Contractors are subject to, at a minimum, a National Agency Check with Local Agency and Credit Checks (NACLIC). Regarding Civilians, depending upon the designation of the position, additional agency checks may be required. For example, Non-Sensitive/IT-III positions are subject to a National Agency Check with Inquiries (NACI); Non-Critical Sensitive/IT-II positions are subject to an Access National Agency Check with Inquiries (ANACI); and Critical-Sensitive/IT-I positions require a favorably completed and adjudicated SSBI or SSBI-PR.

(3) Review command policies and procedures to protect all classified information in the command's charge from unauthorized access or disclosure.

Subj: INFORMATION PROTECTION PROGRAM (SHORT TITLE: IP PROGRAM)

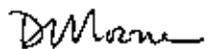
e. Cybersecurity

(1) All MARFORRES Cybersecurity workforce personnel will be qualified in their positions based on the category and level defined by reference (e).

(2) Commanders will ensure annual Information Assurance (IA) and Personally Identifiable Information (PII) training takes place and is reported via the chain of command. The training is available at the following link: <http://iase.disa.mil/eta.index.html>.

(3) In the near future, MARFORRES G-6 Cybersecurity Branch will develop a training plan to ensure execution of specific training and certification requirements mandated by reference (e).

(4) Cybersecurity Workforce Improvement Program tracking, training, and certification will be reported to Headquarters Marine Corps Command, Control, Communication, and Computers on a quarterly basis.


D. L. MOORE

Directives issued by this Headquarters are published and distributed electronically. Electronic versions of the Force directives can be found at:

<http://www.marines.mil/unit/marforres/MFRHQ/G1/Adjutant/ForceOrders/default.aspx>