



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:

5500

ARS

10 APR 2017

Security Note 02-17

From: Director, Administration and Resource Management Division

Subj: HEADQUARTERS, U. S. MARINE CORPS, SECURITY EDUCATION, TRAINING,
AND AWARENESS PROGRAM

Ref: (a) DOD M-5200.01
(b) SECNAV M-5510.30
(c) SECNAV M-5510.36
(d) MCO 5510.18B
(e) HQMC IPSP SOP

1. Per the references, this Security Note outlines the purpose and provisions of the Headquarters U. S. Marine Corps (HQMC) Security Education, Training, and Awareness Program (SETAP). The HQMC SETAP provides the necessary fundamentals to enable quality performance of Staff Agency/Activity security program management. The program instills and maintains a continuous awareness of security requirements and familiarizes personnel with requirements to protect classified information from exposure to unauthorized persons, persons without a valid need to know, and reporting requirements listed in the references. All briefs, forms, and websites mentioned in this Security Note are available at <http://www.hqmc.marines.mil/ar/Branches/Security-Programs-and-Information-Management/>

2. The minimum requirements of the HQMC SETAP are outlined as follow:

a. Initial Orientation Brief. The protection of government assets, people, and property are the responsibility of all personnel. An Initial Orientation Brief will be given to all military, civilian, and contractor personnel upon arrival to HQMC. The Staff Agency/Activity Security Coordinator will fulfill this requirement when personnel check-in. Access to classified material will not be granted until this briefing has been completed. Completion of this orientation will be recorded in Electronic Security Services Request Portal (ESSRP) by the Staff Agency/Activity Security Coordinator and the completion certificate maintained for the duration of the individual's assignment to HQMC.

b. Security Awareness Bulletins. The purpose of a Security Awareness Bulletin is to promote security awareness and compliance with security procedures. These bulletins address security developments, threats, training aids, and resources as they emerge. The increased awareness is intended to help improve the overall security posture. Security Awareness Bulletins are sent from Security Programs and Information Management Branch (ARS) to the Staff Agency/Activity Security Coordinators via email.

c. Annual Training and Briefings

(1) Annual Refresher Brief. The Annual Security Brief must be completed each year by all HQMC personnel to enhance security awareness. This brief reinforces the policies and procedures covered in the initial orientation brief. Completion of the refresher brief will be recorded in ESSRP by the Staff Agency/Activity Security Coordinator and the completion certificate maintained for the duration of the individual's assignment to HQMC.

Subj: HEADQUARTERS, U.S. MARINE CORPS SECURITY EDUCATION, TRAINING,
AND AWARENESS PROGRAM

(2) Counterintelligence Awareness and Reporting (CIAR) Training. The CIAR training covers foreign intelligence threat and methods, including use of the internet and social networking services, insider threats, reportable information, behavior indicators, and reporting procedures. In accordance with Department of Defense (DoD) Directive 5240.06, HQMC personnel are required to receive annual CIAR training in person by a Naval Criminal Investigative Service (NCIS) Agent. Training dates and location will be published by the Director, Administration and Resource Management Division, ARS via separate correspondence.

(3) Antiterrorism Awareness Training. Antiterrorism Awareness Training is the basic knowledge of a terrorist threat and the measures used to reduce personal vulnerability. In accordance with MARADMIN 084/12, all HQMC personnel are required to complete Level I Antiterrorism Awareness Training annually. Level I Antiterrorism Awareness Training is available via MarineNet, code (JATLV10000) or Joint Knowledge Online, code (JS -US007).

(4) Information Assurance (IA) Training. IA protects and defends information and information systems by safeguarding their availability, integrity, authenticity, and confidentiality. In accordance with MARADMIN 330/16, all HQMC personnel must participate in fiscal year IA training. Uniformed personnel will complete MarineNet training curriculum "USMC Cyber Awareness Training", code (CYBERM0000). Civilians will complete all annual cyber awareness training in Total Workforce Management System (TWMS). The courses are titled "DOD Cyber Awareness Challenge V3" and "Privacy and Personally Identifiable Information (PII) Awareness Training". Contractor personnel will complete MarineNet training curriculum "Civilian Cyber Awareness Training", code (CYBERC).

d. Special Training and Briefing. Special training and briefings are occasionally required for select HQMC personnel. These include the following:

(1) Original Classification Authority (OCA) Training. OCAs receive training in the proper classification and declassification of classified national security information with an emphasis on the avoidance of over-classification. Training for newly appointed OCAs shall be provided prior to exercising of the authority and each OCA shall receive training annually thereafter. In coordination with the HQMC Security Manager, the OCA will certify in writing that the training has been received.

(2) Derivative Classifier Training. Derivative classifier training shall be completed and documented initially for anyone within a command who has access to classified information and biennially thereafter for as long as the individual has access to classified information. If refresher training is not conducted within 24-months, derivative classifiers are not authorized or allowed to derivatively classify information until the training is completed. Completion of the derivative classifier training will be recorded in ESSRP by the Staff Agency/Activity Security Coordinator and the completion certificate maintained for the duration of the individual's assignment to HQMC.

(3) North Atlantic Treaty Organization (NATO) Brief. All personnel who require "Access" to NATO classified information based on need-to-know, shall receive a security briefing and sign an acknowledgement on their responsibilities for the protection of NATO information. At no time will access be granted for "just in case" purposes. When requesting access to NATO classified information, a completed NATO Briefing Certificate will be submitted via ESSRP by the Staff Agency/Activity Security Coordinator. The Staff Agency/Activity Security Coordinator will maintain the completion certificate for the duration of the individual's assignment to HQMC.

(4) Foreign Travel Brief. Prior to conducting foreign travel (personal or business), all military, civilian, and DoD contractor personnel must complete a Notification of Foreign Travel Form and the

Subj: HEADQUARTERS, U.S. MARINE CORPS SECURITY EDUCATION, TRAINING,
AND AWARENESS PROGRAM

Foreign Travel Briefing. Personnel must contact their Staff Agency/Activity Security Coordinator to obtain the Notification of Foreign Travel Form.

(5) Hand-Carry Brief. Appropriately cleared personnel may request to escort or transport classified material between locations when other means of transmission cannot be used. Personnel authorized to hand-carry classified material must be informed of the security responsibilities by executing an "Agreement to Hand-Carry Classified Material" given by their Staff Agency/Activity Security Coordinator. The agreement will be kept and maintained by the Staff Agency/Activity Security Coordinator for the duration of the individual's assignment to HQMC.

(6) HQMC Security Manager In-Call Brief. The Staff Agency/Activity Security Coordinators/Assistant Security Coordinators are the principal Information and Personnel Security Program (IPSP) advisors to the Staff Agency/Activity Head. All newly appointed Staff Agency/Activity Security Coordinators will meet with the HQMC Security Manager for an "In-Call" to review policy, address responsibilities, and to ensure Security Coordinators are provided with the necessary skill sets and knowledge to manage the Staff Agency/Activity IPSP proficiently.

(7) USMC Security Management Course. This is the primary course for security management training based on the references and is designed to be USMC specific. The course is open to all positions within command security management programs. For additional information and course requirements visit the PPO PSS Blog site at <https://eis.usmc.mil/sites/hqmcppo/PS/PSS/Blog/default.aspx>.

(a) In order to gain access to the site, users will require a MCEITS account. If you already have a MCEITS account, contact the USMC IPSP Training Program Manager at (703) 692-0157.

(b) If you do not have a MCEITS account, request a MCEITS account via the website at <https://mceits.usmc.mil/SitePages/MCEITS%20Account%20Request.aspx> and select HQMC PPO. Account approval and access to the PSS Blog, will be granted within 72 hours. If after 72 hours, the account has not been created, contact the USMC IPSP Training Program Manager.

(8) Annual Communication Security (COMSEC) Training. Annual COMSEC Training is taken by the Local Element Coordinators (LECO) and Security Coordinators who are assigned LECO duties and the responsible personnel designated by the Staff Agency/Activity Head for administration, accounting, handling, safeguarding and destruction of COMSEC material within their respective Staff Agency/Activity accounts. HQMC ARSC KMI Managers will provide the LECO/Security Coordinator annual COMSEC training. LECO must also complete the Basic COMSEC User Training as described in the below paragraph, 2.d.(9).

(9) Basic COMSEC User training. Personnel identified as COMSEC Users must complete the Basic COMSEC User training at least 10 days prior to signing a Communications Material Security Systems (CMS) Acknowledgment form and annually thereafter.

(10) Security Professional Education Development Program (SPeD). The SPeD Certification Program is intended to ensure that there is a common set of competencies among security practitioners that promote interoperability, facilitates professional development and training, and develops a workforce of certified security professionals. Additional information on the SPeD certification program can be found on the Center for Development of Security Excellence site.

(11) Termination Statement. The Termination Statement informs individuals of their continuing security responsibilities after access and assignment to the Department of Defense has terminated (e.g.


Subj: HEADQUARTERS, U.S. MARINE CORPS SECURITY EDUCATION, TRAINING,
AND AWARENESS PROGRAM

retirement or separation). A Termination Statement is accomplished on the individual's last day of work or when access to classified information is no longer required. Staff Agency/Activity Security Coordinator will conduct the termination briefing and submit the completed Termination Statement via ESSRP.

(12) Sensitive Compartmented Information (SCI). The Special Security Officer (SSO) is responsible for briefing those individuals requiring access to SCI. To schedule a briefing, contact the HQMC SSO at (703) 614-3350.

3. Questions regarding this Security Note should be directed to the HQMC Security Manager at (703) 614-3609.

4. This Security Note supersedes Security Note 07-13.


J. R. NEWELL
By direction