UNITED STATES MARINE CORPS
HEADQUARTERS AND SERVICE BATTALION
MARINE CORPS BASE QUANTICO
2006 HAWKINS AVENUE
QUANTICO, VIRGINIA 22134

IN REPLY REFER TO
5510
B 07-1
7 Feb 2020

Battalion Order 5510.1

From: Commander, Headquarters and Service Battalion
To: Distribution List A

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) MCBO 5510.1D w/CH1 Information and Personnel Security Program
(b) DoD M-5200.01 v. 1-4 DoD Information Security Program
(c) SECNAV M5510.36 Information Security Program
(d) SECNAV M-5510.30 Personnel Security Program
(e) MCO 5510.18B Marine Corps Information and Personnel Security Program
(f) DoD 5200.02 Personnel Security Program

Encl: (1) HQSVC Bn Standard Operating Procedures

1. Purpose. References (a) through (f) requires commanders to establish Information and Personnel Security Programs (IPSP). The purpose of this Order is to establish procedures regarding the management of the Headquarters and Service Battalion (HQSVC Bn) IPSP. All personnel assigned to HQSVC Bn Headquarters and Company Offices (Here in after "Command Post") will comply with this policy.

2. Cancellation. Policy Letter 3-16.

3. Mission. HQSVC Bn establishes an IPSP for HQSVC Bn Command Post (CP) in order to implement and comply with the Department of the Navy and the Marine Corps Personnel Security Programs.

4. Execution

a. Commander's Intent. This policy provides guidance and procedures to ensure that information classified under the authority of Executive Order 13526 is protected from unauthorized disclosure and that only military personnel with an appropriate security clearance and a need to know are granted access to classified information.

b. Concept of Operations. HQSVC Bn will utilize references (a) through (f) to guide its IPSP. HQSVC Bn's IPSP provides implementing guidance and procedures. Subordinate companies and battalion staff will adhere to the program under the cognizance of the Command Security Manager.

c. Tasks

(1) Company Commanders

(a) Review and become familiar with the references and this Order.

(b) Ensure CP personnel comply with this Order and the training requirements contained in the references.

(2) Command Security Manager

(a) Manage the battalion IPSP.

(b) Manage all Personnel Security Investigation matters for the command.

(c) Implement and manage the Security Education Program to instruct personnel in security policies and procedures.

(d) Ensure persons traveling to foreign countries receive a foreign travel brief prior to departure if required by the Naval Criminal Investigative Service.

(e) Manage the Classification Management process.

d. Coordinating Instructions. All military, civilian, and government contractor personnel assigned to HQSVC Bn CP will comply with the provision of this policy. This policy does not address every conceivable circumstance that may arise in routine operations. For any situtation not covered, the basic principles of security management coupled with sound judgement, guidance from appointed security personnel, and common sense should be exercised.

5. Administration and Logistics

a. Administration. Recommendations regarding the contents of this policy may be forwarded to the Command Security Manager, via the HQSVC Bn chain of command.

b. Logistics. The battalion staff will assist in the overall support requirements for training as outlined by this policy.

6. Command and Signal

a. This policy is effective the date signed.

b. This policy is applicable to all HQSVC Bn CP personnel, MCB Quantico.

c. The point of contact for this policy is the HQSVC Bn Security Manager.

E. J. DANIELSON

Headquarters and Service Battalion Information and Personnel Security Program Standard Operating Procedure

Table of Contents

Responsibilities

1. Commanding Officer. Per reference (a), the Commanding Officer is responsible for the formulation, implementation and enforcement of information, personnel, industrial security programs, their effectiveness, and compliance with all directives issued by higher authority.

2. Security Manager/Assistant Security Manager. Per reference (a), the Security Manager/Assistant Security Manager are the principal advisors for information, personnel, security education, and training within this headquarters. The Security Manager/Assistant Security Manager is responsible for:

a. The management, formulation, implementation and enforcement of security policies and procedures for the protection of classified information originated by or under the cognizance of Headquarters and Service Battalion or its infrastructure, in connection with the duties outlined in reference (a).

b. Developing basic policy and procedures for the classification, dissemination, transmission, control, accounting, storage, and protection of collaterally classified information at HQSVC Bn if and when required.

c. Ensuring all personnel under their cognizance comply with the references and this SOP.

d. Ensuring that the Commander of Headquarters and Service Battalion is notified of all:

(1) Instances involving loss, compromise, or compromise of classified information.

(2) Information Technology (IT) system spillages (i.e., inappropriate levels of classified information are introduced to an unclassified or classified non-SCI IT System).

Program Management

1. Guidance or Interpretation. Individual requests for guidance or interpretation of this SOP are encouraged. Address all requests to the Command Security Manager, HQSVC Bn.

2. Training

a. On-the-Job-Training. On-the-Job-Training is the phase of security education when security procedures for the assigned position are learned. Security coordinators will assist supervisors in identifying appropriate security requirements. Supervisors are ultimately responsible for procedural violations and infractions that result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable. This training does not require reporting outside the HQSVC Bn CP but must be recorded within the Command Security Manager's records.

b. Derivative Classifier Training. Personnel who perform derivative classification must complete Derivative Classification Training every two years. The training is available online at the Defense Security Service website, at http://www.cdse.edu/catalog/information-security.html.

3. Briefings.

a. Counterintelligence Awareness. Personnel attached to HQSVC Bn will receive briefings on all threats posed by foreign intelligence and terrorist organizations annually, or as needed due to operational need. These briefings will be scheduled annually, delivered in person by an agent of the NCIS, and reported by the delivering agent. Rosters of attendees to these briefings will be maintained on hand by the HQSVC Bn Security Manager for two years.

b. Special Briefings. Special briefings are occasionally required for select personnel in receipt of appropriate orders or for going abroad. These include the following:

(1) Foreign Travel Briefing. Prior to conducting foreign travel (personal or business), all military, civilian and DoD contractor personnel must receive a foreign travel briefing. Personnel can schedule a briefing from NCIS, at (703)784-4675 or they can contact the HQSVC Bn ATO.

(2) Counter-intelligence Briefing. Upon return from foreign travel outside of the continental United States, members are required to report any suspicious contact to the NCIS for determination and/or matter of record keeping as may be required. Personnel can report suspicious contact to the NCIS at (703)784-4675.

4. Joint Personnel Adjudication System (JPAS) Accounts. Per Reference (d), all Security Managers will have access to JPAS User Accounts. Requests for additional user accounts will be made to MCINCR-MCBQ Security Manager. Personnel requesting a JPAS account must have a need to access JPAS, have current Information Assurance/Cyber Security training, and have taken the JPAS training provided prior to being issued an account. JPAS accounts for users will be terminated upon departing the Command or when they no longer have a need to access the site. JPAS will be utilized for the following:

a. Maintenance of the Command's Personnel Security Management Network (PSM Net). All personnel belonging to HQSVC Bn will need to be properly joined within the HQSVC Bn PSM Net. The HQSVC Bn Security Management Office (SMO) identifier is 300026HS. All personnel attached to the Command will be "owned" or "serviced" by the Security Manager/Assistant within JPAS, as appropriate.

b. Tracking Eligibility. The Security Manager/Assistant is responsible for ensuring that Command personnel have the necessary investigation as required by their position upon checking into the command. Additionally, HQSVC Bn Security Manager/Assistant is required to run reports at least quarterly to identify personnel requiring a security re/investigation. Personnel identified as requiring a PSI will be forwarded to MCINCR/MCBQ Security Manager/Assistant in order to process their PSI.

c. Receiving Correspondence from the Central Adjudication Facility. The HQSVC Bn Security Manager/Assistant is required to review all correspondence sent to the SMO within the Defense Information System for Security (DISS). Categories include but are not limited to: eligibility change, action by servicing SMO, message from CAF, RRU Response, etc.

d. Submitting Visit Requests. JPAS is utilized to send and receive visit requests from one security office to another. Submitting a visit request allows the receiving security office to review the subject's eligibility/access. Visit requests are submitted to SMOs, not individual Security Managers.

e. Submitting Incident Reports. See paragraph 4 under Personnel Security on page 6.

5. Records Disposition. The following instructions are provided:

a. Appointment Letters. Appointment letters for Command Security Managers and the assistants will be retained for a period of two years after the individual assignment has been terminated. Members considered for appointment to these positions should have a minimum of 12 months remaining at the command.

b. Inquiries and Investigations. Reports of completed Inquiries and Investigations will be retained for two years. This includes but is not limited to correspondence pertaining to security violations, infractions, incidents, hazards, or deficiencies in the HQSVC Bn Command Post (CP).

Personnel Security

1. Access. Knowledge or possession of classified information is authorized only for those whose duties require access. Employees will not be allowed knowledge or possession of classified information unless conditions outlined in reference (d) have been met. No employee or personnel will have access to classified information solely because of rank or position.

2. Personnel Security Investigation. No individual will be given access to classified information or be assigned to sensitive duties unless a favorably adjudicated personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations. PSI requirements and definitions are further described in Reference (d).

3. Continuous Evaluation Program (CEP). When questionable, derogatory or unfavorable information becomes available concerning an individual who has been granted access to classified information, or who has eligibility to classified information or is assigned to sensitive duties, this information will be reported to the cognizant Security Manager/Assistant by the HQSVC Bn Security Manager/Assistant.

a. Individuals are ultimately responsible to report to their supervisor or their Command Security Manager/Assistant and seek assistance for any incident or situation that could affect their continued eligibility for access/eligibility to classified information.

b. Marines have an obligation to advise their Chain of Command or Command Security Manager/Assistant when they become aware of information which falls within the 13 adjudicative guidelines. The following guidelines are defined in Reference (d).

(1) Allegiance to the United States

(2) Foreign influence

(3) Foreign Preference

(4) Sexual Behavior

(5) Personal Conduct

(6) Financial Considerations

(7) Alcohol Consumption

(8) Illegal or improper drug use/involvement

(9) Psychological Conditions

(10) Criminal Conduct

(11) Handling Protected Information

(12) Outside Activities

(13) Use of Information Technology

4. Incident Reports

a. For Marines who fall under the HQSVC Bn Command Post, when derogatory information is brought to the attention of the HQSVC Bn Security Manager the following steps will be taken:

(1) The information will be reported to the MCINCR-MCBQ Security Manager/Assistant, who will advise the most appropriate course of action in submitting the information to the DoD Consolidated Adjudications Facility (CAF) via DISS or the DoD CAF Portal.

(2) All pertinent information and documentation will be sent to the CAF via the DISS portal or through direct email contact with the CAF adjudicator assigned to the subject's case, and is required to be maintained for a period of two years after the individual has departed the Command.

(3) The HQSVC Bn Security Manager will inform the MCINCR-MCBQ Security Manager/Assistant in the issuance of or derogatory determination from the CAF to include but not limited to:

(a) Letter of Intent (LOI)

(b) Statement of Reasons (SOR)

(c) Conditional Security Clearance

(d) Warning Letter

(e) Denied eligibility

(f) Withdrawn eligibility

(g) No Determination Made

b. For all Marines who are under the administrative control of HQSVC Bn, when derogatory information is brought to the attention of the HQSVC Bn Security Manager the following steps will be taken:

(1) The supported organization's SMO that the Marine with derogatory information falls under will be notified.

(2) The notification will include a general explanation of the situation and if necessary the contact information of the HQSVC Bn Legal Office so that continued coordination can be provided as the situation develops.

(3) The supported organization's SMO is responsible for all coordination and communication with the CAF.

5. Check-ins. All personnel assigned to HQSVC Bn who receive security service support must check-in with the HQSVC Bn Security Manager/Assistant. The Security Manager/Assistant will establish the appropriate relationship within JPAS while also verifying the subject's security investigation and clearance status. In addition, any security orientation and in-briefing will occur at this time.

6. Check-out/Debriefings

a. All personnel who are assigned to HQSVC Bn must complete a security check-out prior to departing. The HQSVC Bn Security Manager/Assistant will ensure all personnel departing the HQSVC Bn Command Post complete the following:

(1) Military Personnel Checkout

(a) Receive the HQSVC Bn Command Debriefing.

(b) Check the member out of the Command's Personnel Security Management Network (PSM Net) within JPAS.

(c) Remove any access to classified information within JPAS.

(d) If the individual is retiring or separating, have them complete the security termination statement which is to be forwarded to MMSB for indefinite retention at the following address:

CMC
HQMC (MMSB-20)
M&RA
2008 Elliot Road
Quantico, VA 22134-5030

(e) If the subject has been issued a courier card, collect and forward to the MCINCR-MCBQ Information Security Officer.

(2) Civilian Personnel Checkout

(a) Receive the HQSVC Bn Command Debriefing.

(b) Check the member out of the Command's PSM Net within JPAS.

(c) Remove any access to classified information within JPAS.

(d) If the individual is retiring or leaving federal civil service, have them complete the security termination statement which is to be forwarded to OCHR for indefinite retention at the following address:

OCHR San Diego Operations Center
Code 522
PO Box 452015, Bldg 6300 Miramar Way
San Diego, CA 902145-2015

(e) If the subject has been issued a courier card, collect and forward to the MCINCR-MCBQ Information Security Officer.

b. Security Manager/Assistant will retain a local copy of Security Debriefing Forms for two years from date of checkout. Security Debriefing Forms are items subject to inspection.

7. Courier Cards. To request a courier card for Command personnel, the Security Manager/Assistant will submit a request to the MCICNR-MCBQ Information Security Officer (ISO) indicating what type of courier card (i.e. NCR, CONUS, and OCONUS), level of access required and a duration (not to

exceed two years). All personnel that are issued a courier card must read and acknowledge their responsibilities for escorting or hand carrying classified information. Upon departing the command or when no longer required, the courier card will be turned into the HQSVC Bn Security Manager/Assistant or the MCINCR-MCBQ ISO.