UNITED STATES MARINE CORPS
11TH MARINES
BOX 555503
CAMP PENDLETON, CA 92055-5503

5510
SecMgt
28 May 20

REGIMENTAL POLICY LETTER 5-20

From: Commanding Officer
To: All Hands

Subj: COMMAND SECURITY INSTRUCTION

Ref: (a) Executive Order 13526
(b) Intelligence Community Classification and Control Marking Implementation Manual
(c) Marking Classified National Security Information Booklet
(d) DOD Manual 5200.01, Vol 1-4 DOD Information Security Program
(e) DOD 522022M National Industrial Security Program Operating Manual
(f) DODD 5240.06 Counterintelligence Awareness and Reporting
(g) DOD Instruction O-5240.21 Counterintelligence Inquiries
(h) SECNAV M-5510.36 DON Information Security Program
(i) SECNAV M-5510.30 DON Personnel Security Program
(j) SECNAVINST 5510.37 DON Insider Threat Program
(k) JAGINST 5800.7D Manual of the Judge Advocate General
(l) MCO P5510.18B USMC Information and Personnel Security Program Manual
(m) MCO 5530.14A Physical Security Program Manual
(n) USMC Security Management Handbook
(o) IMEFO P5510.1D Security Instruction
(p) DivO P5510.13H
(q) 11th Marines Regimental Inspection Program
(r) 11th Marines Emergency Action Plan for Classified Material Control Center and Electronic Key Management System and Emergency Destruction Plan
(s) 11th Marines Communications Security Standard Operating Procedures
(t) 11th Marines Designation of Restricted Areas

Encl: (1) Command Security Instruction Periodic Actions

1. Purpose. To establish the information and personnel security program (IPSP) within 11th Marines in accordance with the references.

2. Action. Commanders are directly responsible for safeguarding all classified material within their command and educating personnel in security practices and procedures in connection with the handling and control of classified material. Commanders will develop their own command security instructions in accordance with the references. All personnel in this regiment will ensure compliance with the provisions of this order.

3. Recommendations. Recommendations, comments, and inquiries concerning this order are solicited and should be submitted to the regimental assistant security manager, Captain Daniel Williams, at (760)725-3885 or daniel.i.williams@usmc.mil.

R. MIAGANY

LOCATOR SHEET

Subj: COMMAND SECURITY INSTRUCTION

Location: _____
(Indicate the location(s) of the copy(ies) of this order)

CONTENTS

CHAPTER 1

COMMAND SECURITY MANAGEMENT

1. Purpose. This order establishes the information and personnel security program (IPSP) for 11th Marines. The purpose of the IPSP is to protect national security information from unauthorized disclosure or loss. This order is intended to supplement, not replace, the references and must be used in conjunction with those directives to be effective.

2. Applicability. This order applies to all 11th Marines units and personnel. Commanders are directly responsible for safeguarding all classified materials within their commands and educating personnel in security practices and procedures in connection with the handling and control of classified material. Commanding officers at the battalion level are specifically directed to develop their own command security instructions in accordance with the references.

3. Chain of Command. The security chain of command is as follows:

a. Commanding Officer

b. Security Manager

c. Assistant Security Manager

d. Security Assistant(s)

4. Security Positions.

a. Commanding Officer. For the purposes of this order, "Commanding Officer" refers to O-5 and O-6 Commanding Officers in 11th Marines. The Commanding Officer is overall responsible for compliance with and implementation of the IPSP. The Commanding Officer, 11th Marines, has not been delegated original classification authority. Commanding Officers will, in accordance with the references:

(1) Be the subject of a favorably adjudicated single scope background investigation (SSBI) or Tier 5 (T5) investigation, completed within the last six years.

(2) Designate a Security Manager in writing.

(3) Designate an Information Systems Security Manager (ISSM) in writing.

(4) Designate a Security Officer/Physical Security Officer in writing to manage facilities security.

(5) Issue a written Command Security Instruction.

(6) Ensure that the Security Manager and other command security professionals are appropriately trained, that all personnel receive required security education and that the command has a robust security awareness program.

(7) Prepare an emergency action plan for the protection of classified material in conjunction with an emergency destruction plan to include "in extremis" measures for classified material destruction.

(8) Ensure that command security inspections, program reviews, and assist visits to subordinate commands are conducted at least annually.

b. Security Manager. The Security Manager is the principal advisor on information and personnel security in the command and is responsible to the Commanding Officer for the management of the program. The Security Manager for 11th Marines is the Executive Officer. In accordance with the references, command security managers will:

(1) Be afforded direct access to the Commanding Officer to ensure effective management of the command's security program.

(2) Be an officer or civilian employee (GS-11 or above) with sufficient authority and staff to manage the program for the command, be a U.S. citizen and be the subject of a favorably adjudicated SSBI or T5 investigation, completed within the last six years (Secured Compartmented Information eligibility not required).

(3) Be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc.

(4) Be formally trained on their duties as Security Manager in accordance with HQMC IPSP.

(5) Serve as the Commanding Officer's advisor and direct representative in matters pertaining to the classification, safeguarding, transmission and destruction of classified information.

(6) Serve as the Commanding Officer's advisor and direct representative in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

(7) Develop written command information and personnel security procedures, including an emergency plan which integrates the emergency destruction plan when required.

(8) Formulate and coordinate the command's security awareness and education program.

(9) Ensure security control of visits to and from the command when the visitor requires, and is authorized, access to classified information.

(10) Ensure that all personnel who will handle classified information or will be assigned to sensitive duties are appropriately cleared through coordination with the Department of Defense Central Adjudication Facility (DOD CAF) and that requests for personnel security investigations (PSIs) are properly prepared, submitted and monitored.

(11) Ensure that access to classified information is limited to those who are eligible and have the need-to-know.

(12) Ensure that Personnel Security Investigations (PSIs), clearances, and accesses are properly recorded.

(13) Coordinate the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(14) Coordinate with the command ISSM on matters of common concern.

(15) Ensure that all personnel who have had access to classified information who are separating, retiring, or relieved for cause have completed a Security Termination Statement (STS). Security Termination Statements will be forwarded to Headquarters Marine Corps (HQMC).

(16) Ensure all personnel execute a classified information nondisclosure agreement (SF-312) prior to granting initial access to classified information. SF-312s will be forwarded to Headquarters Marine Corps (HQMC).

(17) Ensure that all personnel that have access to classified information complete derivative classification training through Joint Knowledge Online (JKO) annually and provide their completion certificate to the Assistant Security Manager or Security Assistants.

(18) Ensure that command security personnel are utilizing the Joint Personnel Adjudication System (JPAS) or (Defense Information System for Security (DISS) as required, including:

(a) Proper establishment of the Security Management Office (SMO).

(b) Proper establishment of the Personnel Security Management Network (PSM Net).

(c) Proper establishment of the parent relationship with higher headquarters.

(d) The Security Manager and Assistant Security Manager (if applicable) assigned as JPAS account managers.

(e) Elements of the continuous evaluation program reported as incidents.

c. Assistant Security Manager. The Assistant Security Manager assists the Security Manager in all duties listed above. The Assistant Security Manager for 11th Marines is the Intelligence Officer. In accordance with the references, Assistant Security Managers will:

(1) Be a U.S. citizen, and either a Staff Sergeant (E-6) or above, or a civilian GS-6 or above.

(2) Be designated in writing by the commander to sign SF-312s on behalf of the United States Government.

(3) Be the subject of a favorably adjudicated SSBI/T5 within the last six years if they are designated to issue interim clearance/temporary access. Otherwise, the investigative and

clearance requirements will be determined by the level of access to classified information required.

(4) Assist the Security Manager in all duties listed in paragraph b. above.

d. Security Assistant(s). Civilian employees and military members performing administrative functions under the direction of the Security Manager and/or Assistant Security Manager may be assigned without regard to rank or grade as long as they have the clearance needed for the access required to perform their assigned duties and tasking.

e. Information Systems Security Manager (ISSM). Each command involved in processing data in an automated system, including access to local area networks and/or INTRANET/INTERNET, must designate a civilian or military member as an ISSM. The ISSM is responsible to the Commanding Officer for development, maintenance, and implementation of the information security (INFOSEC) program within the activity. The ISSM advises the Commanding Officer on all INFOSEC matters, including identifying the need for additional INFOSEC staff. The ISSM serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. The ISSM for 11th Marines is the Communications Officer.

5. Inspections, Assist Visits, and Reviews. Commanding officers are responsible for evaluating the security posture of their subordinate commands. Per reference (h), inspections will be conducted annually.

a. Per reference (q), 11th Marines will conduct inspections of Commanding General's Inspection (CGI) Functional Area (FA) 5510.3 IPSP annually with August the preferred month to conduct the inspection. The 11th Marines security manager will conduct inspections of each battalion and the regiment itself in accordance with reference (q), and will also conduct an internal review of security procedures, this instruction, and the security manager turnover binder. All battalion inspections will be maintained for inspection purposes and for review prior to any assist visits or CGI.

b. 11th Marines security management team will conduct assist visits prior to any 11th Marines battalion undergoing a CGI once properly coordinated and requested from the battalion security manager. 11th Marines may request an assist visit from adjacent regiments or from 1st Marine Division as required to ensure complete compliance with all references.

CHAPTER 2

SECURITY EDUCATION

1. Purpose. The purpose of the command security education program is to ensure that all personnel understand the need and procedures for protecting classified information and increasing security awareness for personnel. The goal is to develop fundamental security habits as a natural element of each task.

2. General Requirements. Security education must be provided to all personnel annually. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command. An example security training brief is provided on the HQMC Security Division SharePoint site. Minimum requirements of the security education program are the following:

a. Advise personnel of the adverse effects to national security which could result from unauthorized disclosure of classified information and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control.

b. Advise personnel of their responsibility to adhere to the standards of conduct (see reference (j), Appendix F) required of persons holding positions of trust and to avoid personal behavior which could render them ineligible for access to classified information or assignment to sensitive duties.

c. Advise personnel of their obligation to notify their supervisor or Command Security Manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties.

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties.

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material and alert them to the strict prohibitions against improper use and abuse of the classification system.

f. Familiarize personnel with the procedures for challenging classification decisions believed to be improper.

g. Familiarize personnel with the security requirements for their particular assignments and identify restrictions.

h. Instruct personnel having knowledge, possession, or control of classified information how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her official duties, and can properly protect (store) the information.

i. Advise personnel of the strict prohibition against discussing classified information over an unsecured telephone or in any other manner that may permit interception by unauthorized persons.

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information.

k. Inform personnel of their particular vulnerability to compromise during foreign travel.

l. Advise personnel that they are to report to their Commanding Officer, activity head or designee, contacts with any individual regardless of nationality, whether within or outside the scope of the individuals official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information, or

(2) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

m. Advise personnel of the penalties for engaging in espionage activities and for mishandling classified information or material.

n. Indoctrinate personnel upon employment by the Department of the Navy (DON) in the basic principles of security.

o. Orient personnel who will have access to classified information at the time of assignment, regarding command security requirements.

p. Provide on-the-job training in specific security requirements for the duties assigned.

q. Provide annual refresher briefings for personnel who have access to classified information.

r. Coordinate counterintelligence awareness and reporting (CIAR) refresher training every year for personnel. Per reference (f), CIAR training should include:

(1) The threat from foreign intelligence entities (FIEs).

(2) The methods, also known as "modus operandi," of FIEs.

(3) FIE use of the internet and other communications including social networking services.

(4) The counterintelligence insider threat.

(5) Anomalies in accordance with references (b) and (g).

(6) Reporting responsibilities regarding foreign travel and foreign contacts.

(7) Reporting requirements per reference (f), enclosure (4).

s. Provide special briefings as circumstances dictate.

t. Debrief personnel upon termination of access.

3. Requirements for Security Personnel. Additional security education and training is required for security personnel.

a. Security Managers (and Assistants). The commanding officer shall ensure that his security manager and his assistant security manager have received appropriate security education and training. Security managers and their assistants shall, as soon as they are able to be scheduled, attend the Security Managers Course; see the HQMC Security SharePoint for scheduling information (https://eis.usmc.mil/sites/hqmcppo/PS/PSS/Blog/default.aspx). Security managers and their assistants shall, within 30 days of their written appointment, complete the following online courses via the DOD Center for the Development of Security Excellence (CDSE) Security Training, Education and Professionalization Portal (STEPP) at http://www.cdse.edu/stepp/:

(1) Introduction to Industrial Security (IS011.16)

(2) Introduction to Personnel Security (PS113.16)

(3) Introduction to Information Security (IF011.16)

(4) Introduction to Physical Security (PY011.16)

(5) Marking Classified Information (IF105.16)

(6) Derivative Classification (IF103.16)

(7) JCAVS User Levels 2-6 (PS183.16)

(8) Insider Threat Awareness (INT101.16)

b. Security Assistant(s). Security assistants should, at a minimum, complete the above prerequisite courses, although it is not required by any other order or instruction.

c. Couriers. Commanding officers shall ensure that couriers are informed of and acknowledge their security responsibilities when escorting or hand carrying classified information. The latter requirement may be satisfied by a briefing or by requiring the courier to read written instructions that contain the information listed below, at a minimum:

(1) The courier is liable and responsible for the information being escorted.

(2) The information is not, under any circumstances, to be left unattended.

(3) During overnight stops, classified information is to be stored at a U.S. embassy, military or appropriately cleared DOD contractor facility and shall not, under any circumstances, be stored unattended in vehicles, hotel rooms or hotel safes.

(4) The information shall not be opened en route except in the circumstances described in chapter 2 subparagraph 3.c.8 of this instruction.

(5) The information shall not be discussed or disclosed in any public place or conveyance.

(6) The courier shall not deviate from the authorized travel schedule.

(7) The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents) are complete, valid, and current.

(8) There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights. Carry-on bags and packages may be subjected to x-raying and inspection by customs or airline/airport security officials. If there is a question about the contents of the package, the courier shall present the courier authorization to the official or to the official's supervisor, if necessary. If the official demands to see the actual contents of the package, it may be opened in his or her presence, in an area out of sight of the general public. However, under no circumstances shall classified information be disclosed. Immediately after the examination, the courier shall request that the package be resealed and signed by the official to confirm that the package was opened. Inform both the addressee and the dispatching security office, in writing, of the opening of the package.

(9) Upon return, the courier shall return all classified material in a sealed package, with receipts for any information that is not returned.

(10) A courier card can be given to the courier for carrying classified material. The courier will not maintain the courier card after conducting duties of transporting and maintaining classified material, and will turn in the courier card to the security management team.

CHAPTER 3

INFORMATION SECURITY

1. Purpose. The purpose of the information security program is to apply uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission, and destruction of classified information. Reference (h) established the DON information security program and is the base document for the 11th Marines information security program. All information security program manners will be handled by the assistant security manager. This chapter establishes local policies that supplement reference (h).

2. Classification and Marking. It is DOD policy to make available to the public as much information as possible, consistent with the need to protect national security. Therefore, information shall be classified only to protect the national security of the United States. The Commanding Officer, 11th Marines, is not a designated original classification authority (OCA). Therefore, all classification and marking of classified information done within the command is on the basis of derivative classification.

a. Derivative Classification. Derivative classification is the incorporating, paraphrasing, restating, or generating, in new form, information that is already classified, and the marking of newly developed information consistent with the classification markings that apply to the classified source. This includes classification guidance or source documents. All DoD personnel, including contractors, who access classified systems and networks or perform derivative classification functions are required to complete derivative classification training annually. (reference Chapter 2 of this order for more information on accessibility). Derivative classifiers shall:

(1) Observe and respect the original classification determinations made by OCAs (and as codified in classified source documents and security classification guides).

(2) Use caution when paraphrasing or restating information extracted from a classified source document(s) to determine whether the classification may have been changed in the process.

(3) Carry forward to any newly created information the pertinent classification markings.

For more information on derivative classification and classification markings, see references (c), (d), and (h).

b. Security Classification Guides. Security classification guides (SCGs) serve both legal and management functions by recording DOD original classification determinations. SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements. For access to relevant DON SCGs, visit http://www.secnav.navy.mil/dusnp/Security/Information/Pages/SecurityClassificationGuides.aspx or contact the security manager.

c. Working Papers. Secret and confidential working papers such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain secret or confidential information shall be:

(1) Dated when created;

(2) Conspicuously marked centered top and bottom of each page with the highest overall classification level of any information they contain along with the words "Working Paper" on the top left of the first page in letters larger than the text;

(3) Protected per the assigned classification level; and

(4) Destroyed, by authorized means, when no longer needed.

For more information on classified working papers, see reference (h), chapter 7.

3. Safeguarding. Commanding Officers shall ensure that classified information is processed only in secure facilities, on accredited information technology (IT) systems, and under conditions which prevent unauthorized persons from gaining access. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified information is processed or stored. These areas will be designated, in writing, by the commanding officer as restricted areas. Areas designated as open storage areas within the command will be subjected to a physical security survey conducted by the security manager, a school trained military occupational specialty (MOS) 5814 physical security specialist, or a civilian physical security specialist. Of note, 11th Marines facilities are not accredited to process or store top secret or top secret/sensitive compartmented information.

a. Secret and Confidential Control Measures. Commanding officers shall establish administrative procedures for the control of secret information appropriate to their local environment, based on an assessment of the threat, the location, and mission of their command. These procedures shall be used to protect secret information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this order and the references. Within 11th Marines, Secret information will be processed and stored only under the following conditions:

(1) In a General Services Administration (GSA) approved container, vault, modular vault, or secure room.

(2) In a properly secured container when being transported by an appropriately cleared and documented courier.

(3) Under 24-hour guard in field conditions, and when not in a General Services Administration (GSA) approved container, vault, modular vault, or secure room.

(4) For classified meetings and conferences, only under the conditions described by reference (e), volume 3, enclosure 2, page 23; and reference (h), paragraph 7-13.

(5) Special types of classified information shall be processed and stored separately from normal Secret information. Those only with a need to know should have access to this information and the information will be safeguarded out of view from those without a need to know.

b. Controlled Unclassified Information. In addition to safeguarding classified information, commanding officers shall ensure that controlled unclassified information (CUI) is safeguarded from unauthorized access by the public. Measures shall be taken to protect IT systems which store, process, and transmit such information from unauthorized access. This includes the marking of systems and media authorized to process CUI. Examples of CUI are information marked For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Limited Distribution (LIMDIS), and North Atlantic Treaty Organization (NATO) Unclassified (//NU). These measures include proper storage in a locked container when not being utilized for authorized purposes. The public shall not be allowed near any areas containing CUI or thought to contain CUI without proper clearance and guidance from the Command Security Manager.

c. Reproduction of Classified and Controlled Unclassified Information. No information shall be reproduced without approval from the Command Security Manager. Originators of this information shall be informed and allowed to place any special controls on the information to safeguard it as needed. Reproduction shall only be done minimally, not in excess, to avoid spillage and/or leaked information to the public. See chapter 3, par 3a and 3b for proper control measures of the information.

d. Care During Working Hours. Classified information will be kept under constant surveillance by an authorized person and covered with classified material cover sheet (SFs 703-705) when removed from secure storage. The S-2 and TAP secure rooms and Electronic Key Management Infrastructure (KMI) vault are approved open storage facilities. Classified discussions shall not be conducted in public conveyances or places that permit interception by unauthorized persons, and classified material may not be opened or read in any area where it can be seen by unauthorized individuals.

e. End-of-Day and Duty Checks. End-of-day checks will be conducted using the SF 701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, and SF 702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms, strong rooms, and security containers have been properly secured at the end of the day. These SFs shall also be annotated to reflect after hours, weekend, and holiday activities. These forms may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation. All open storage secured areas while in a closed status are required to conduct 4 hour checks by duty personnel (regimental command duty officer, battalion officers of the day, or sentry) which includes the S-2 secure room, KMI vault, TAP secure room and subordinate battalion S-2 secure rooms or vaults at a minimum of every four hours, and will log the time on the SF 702 posted on each door ; all closed storage secured areas while in a closed status require 12 hour checks by sentry.

f. Combinations. Safe and door combinations will be stored in alternate locations for reference using the SF 700, Security Container Information, and the appropriate portion of the SF will be affixed to the inside of the container. The S-2 secure room combination is located in the KMI vault and with the subordinate battalion S-2 secure rooms; the EKMS vault combination is stored in the S-2 secure room and the TAP combination is stored in the S-2 secure room. Combinations will be changed in accordance with the provisions outlined in reference (h), paragraph 10-12.

g. Communication and Strategy. Proposed press releases and information intended for the public will be subjected to a security review. The security manager will make coordination with the servicing Communications Strategy (COMMSTRAT) officer, 1st Marine Division, at (760) 725-6573.

h. In Foreign Countries. For information on the safeguarding of classified information located in foreign countries, see reference (h).

i. Information Technology (IT) Systems. All IT systems that are used to process and store Classified information are only utilized on SIPR networks and in a secure room or vault. 11th Marines' secure room contains IT systems that allow for the production, recreation, and distribution of classified information for those that possess the proper clearance and need-to-know. These IT systems will be consistently monitored and secured while not in use. No person will be allowed to utilize these systems on their own unless they are approved by the Command Security Manager and listed under the unit after-hours access roster.

j. Residential Storage. 11th Marines does not allow residential storage to be utilized. However, in the event that it is needed, see reference (h) for all required information.

4. Transmission and Transportation. Commanding officers shall ensure that only appropriately cleared personnel or authorized carriers transmit, transport, escort, or hand carry classified information. The means selected should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance. For information on the transmission and transportation of classified material, see reference (h), chapter 9.

a. Couriers. Commanding officers will ensure that couriers are informed of security responsibilities when escorting or hand carrying classified information. For courier security education and briefing requirements, see chapter 2 of this order.

b. Classified Mail. The 43 Area Postal Facility is owned by Marine Corps Base (MCB) Camp Pendleton. Therefore, standard operating procedures (SOPs) for ensuring proper storage and dissemination of mail that may contain sensitive and/or classified information are maintained at the MCB level. Once 11th Marines receipts for any classified mail, normal safeguarding procedures apply.

5. Dissemination. Unless specifically prohibited by the originator, secret and confidential information originated within the DOD may be disseminated to other DOD components and agencies within the executive branch of the U.S. Government. Classified information and CUI originated or received by the command shall be handled and distributed according to the administrative procedures on page 13.

6. Loss or Compromise. The loss or compromise of classified information presents a threat to the national security of the United States. Reports of loss or compromise ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of the loss or compromise and to preclude recurrence.

a. Definitions.

(1) Loss. A loss of classified information occurs when it cannot be accounted for or physically located.

(2) Compromise. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid security clearance, authorized access, or need-to-know. A possible compromise occurs when classified information is not properly controlled. For the purposes of this order, electronic spillage occurs when data is placed on an information technology system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this chapter.

b. Reporting Requirements.

(1) Commanding Officer. When a loss or compromise of classified information occurs, the cognizant commanding officer or security manager shall immediately initiate a Security Inquiry (SI). The Commanding Officer shall appoint, in writing, a command official, other than the Command Security Manager or anyone involved, either directly or indirectly with the incident, to conduct a SI. If, during the conduct of the SI, it is determined that a loss or compromise of classified information did occur, the Naval Criminal Investigative Service (NCIS) Marine Corps West Field Office will be notified ((760) 725-5158). NCIS shall promptly provide advice and assistance to the SI as necessary. Timely referral to NCIS is imperative to ensure preservation of evidence for any possible counterintelligence matters or criminal investigation.

(2) Security Manager. The security manager shall be responsible for supporting the SI process. In the event of compromise or possible compromise on an IT system, the security manager shall coordinate with the information assurance manager to ensure that these incidents are properly reported in accordance with this order and reference (h). Additionally, the information assurance manager shall ensure that the possibly compromised classified information is sanitized from the affected system(s) in accordance with reference (l) when directed to do so by the security manager or commanding officer.

(3) Individual. An individual who becomes aware that classified information is lost or compromised shall immediately notify their security manager or commanding officer of the incident, as well as their supervisory chain of command. If the reporting individual believes the security manager or commanding officer may be involved in the incident, they must notify the next higher echelon of command or supervision. If circumstances of discovery make such notification impractical, the reporting individual shall notify the commanding officer or security manager at the most readily available command or contact the NCIS Marine Corps West Field Office at (760) 725-5158.

c. For additional guidance on the reporting and investigation of loss or compromise of classified material, see reference (h), chapter 12.

7. Destruction. Classified information will be destroyed when it is no longer required for operational purposes. Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information, too include "in extremis" means of destruction. Commanding officers will establish at least one day each year as a clean out day when specific attention and effort are focused on disposition of unneeded classified

material. The designated clean out days for 11th Marines is 1 April and 1 October each year. If 1 April or 1 October falls on a non-work day, the clean out shall be accounted for prior to that non-work day. 11th Marines S-2 and KMI coordinate to produce an Emergency Destruction Plan for proper destruction of classified material. 11th Marines Electronics Maintenance Platoon (EMP) has the ability to destroy classified and unclassified hard drives and is organic to the unit. Additional facilities that can destroy information include the S-2 Secure Room and 1st Marine Division G-2/G-6. For more information on approved destruction methods and standards, see reference (h), chapter 10.

8. 11th Marines Classified Material Control Center (CMCC) Management. Inspections of Classified Military Information (CMI) will be conducted monthly. A CMCC Officer will be appointed in writing; this is commonly the Adjutant, but can be any officer that is not directly involved in CMI handling to function for unbiased oversight. It will be the responsibility of the section leader to maintain appropriate accountability of their CMI. The section leader can designate, in writing, personnel acting as a Secondary Control Point (SCP) to conduct day-to-day operations. The Security Management team will train the designee and assigned alternative personnel to the designee on how to appropriately manage control of CMI. The Standard Form 153 (SF-153) will document inventory, destruction, check-out for usage, transfers between sections, transfers between secured areas and rooms, and transfers between 11th Marines and outside units. All transactions, even ones lasting the working day only, will require an SF-153. In all SF-153 transactions, to include inventory, two parties must be involved. The SF-153 will be completed digitally with a digital and hard copy maintained on file for no less than three years. A copy of the monthly inventory will be given to the Security Management team and to the CMCC Officer. The battalions will deliver the SF-153 to the regiment (digitally or otherwise) where the regiment will also maintain a copy for no less than three years. If the daily checkout will extend beyond business hours on the day of checkout, an SF-153 transfer must be generated beforehand.

9. Emergency Action Plan and Emergency Destruction Plan. For procedures governing the emergency protection, removal, and destruction of classified material and equipment, see reference (s).

CHAPTER 4

PERSONNEL SECURITY

1. Purpose. The purpose of the personnel security program is to authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties to those persons whose loyalty, reliability, and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of national security. Additionally, the personnel security program ensures that no final unfavorable personnel security determination will be made without compliance with all procedural requirements. The base orders for the personnel security program are references (i) and (j). This chapter is a supplement to those orders.

2. Personnel In-Processing. When personnel check into the unit, the security manager will ensure they are properly checked in using JPAS or DISS. When granting access to classified information, the security manager will make a determination based on the existence of a favorably adjudicated personnel security investigation (appropriate to the level of classified information for which access will be granted), a need to know, and a SF 312. SF 312s will be entered into JPAS and forwarded to manpower management separation and retirement (MMSR). Additionally, the SF 312 pamphlet will be available for review if requested by the individual. As part of personnel in-processing, individuals being granted access to classified information will also be briefed on NATO (see reference (e), volume 1, enclosure 3, paragraph 11(c)). Furthermore, personnel being granted top secret access must complete a personal attestation statement with the 1st Marine Division, Special Security Officer (SSO) (point of contact is (760) 725-5454). Security managers are reminded that, per reference (j), access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on need to know. Additionally, the level of access authorized will be limited to the minimum level required to perform assigned duties. No one has a right to have access to classified information solely because of rank, position, or security clearance.

3. Personnel Security Investigations (PSI). No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability, and trustworthiness. A PSI is conducted to gather information pertinent to these determinations.

a. Constraints and Restraints. Security managers must ensure that PSIs are only initiated for the level of eligibility and access required for individuals per the MOS Manual, unit table of organization (to include matching of billet identification codes (BICs)), or directive from higher headquarters. Initiating a PSI for a level of eligibility and access above that which is articulated by any of these documents (e.g. submitting a Marine for a T5 investigation when he only rates a T3 investigation) constitutes fraud, waste, and abuse. However, all Marines in the command must have been the subject of a National Agency Check with Local Agency Checks and Credit Check (NACLC) or T3 PSI, irrespective of their classified information access requirements, in order to determine enlistment or appointment eligibility. Government civilian employees in the command must have been the subject of a National Agency Check with Inquiries (NACI) PSI irrespective of their classified information access requirements, in order to determine government employment suitability. Personnel employed in or assigned to duties in IT Level I, II, or III positions must have been the subject of the appropriate PSIs (see references (i) and (o) for requirements).

b. Submission. PSIs will be initiated by security personnel via the Office of Personnel Management (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) system. Security managers will conduct periodic reviews of personnel under their purview, via JPAS PSM Net, no less than once per quarter. For more information on PSIs, see references (j) and (o).

c. Appeals. Appeals of DODCAF revocation/denial decisions regarding clearance eligibility will be processed per the provisions of reference (i), chapter 8, including:

(1) Supporting the Marine as an advocate for the appeal.

(2) Ensuring all timelines pertaining to DODCAF, Defense Office of Hearings and Appels (DOHA), and Personnel Security Appeals Board (PSAB) requests for information are met.

(3) Ensuring permanent change of station (PCS) orders are held in abeyance pending the final decision of the appeal.

4. Temporary Access. Per reference (j), temporary access (formerly known as interim clearance) may be granted to DON personnel who have been otherwise determined to be eligible for a security clearance by the DODCAF but do not currently require a security clearance/access to perform assigned duties. Before authorizing temporary access, the commanding officer must determine that it is to the DON's benefit to allow disclosure to an individual who does not require access in the usual performance of his duties. To be clear, temporary access is only to be granted when access to classified information is required; it is not temporary eligibility for reenlistment or assignment purposes. For more information on temporary access, see reference (j), Chapter 9. There are two primary situations in which temporary access may be justified:

a. Personnel who have been otherwise determined to be eligible for a security clearance by the DODCAF but do not currently require a security clearance/access to perform assigned duties.

b. Personnel who are pending receipt of eligibility certification. Per reference (o), personnel in this category must, for temporary secret or confidential access:

(1) Sign the SF 312

(2) Have their temporary access recorded in JPAS

(3) Have their personnel security questionnaire (PSQ) favorably reviewed by the security manager

(4) Have no known disqualifying information (see paragraph 5 of this chapter)

(5) Have a T3 request successfully submitted to OPM (this is reflected by an open investigation in JPAS)

(6) Have a favorable review of local records (including personnel, medical, legal, security, and/or military police).

5. Continuous Evaluation Program. The security manager will ensure that personnel security related information and accesses are properly recorded in JPAS and that local records are kept, if appropriate. In all instances that require a security clearance reinvestigation and are within a year of expiring, the personnel must complete a Standard Form 86 (SF-86). Once the SF-86 is completed, the security management team must review the SF-86 and identify any discrepancies or anomalies that will hinder the ability for the National Background Investigation Bureau (NBIB) to conduct an investigation. Once the review is conducted and there are no corrections needed, the security management team will save the SF-86 as a .xml file and send the file to the 1st Marine Division CMCC. Once the CMCC receives the file, they will send it to the Department of Defense Consolidated Adjudication Facility (DODCAF) for enrollment into the Continuous Evaluation Program. Enrollment into the Continuous Evaluation Program can be checked via each individual profile on DISS.

a. Personnel Security Standards. Personnel security standards are outlined in reference (j), Appendix F. Adjudication guidelines are outlined in reference (j), Appendix G.

b. Reporting Requirements. All personnel are obligated to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties. This includes an obligation to self-report derogatory information vis-à-vis personnel security standards. Personnel who have access to classified information who are either an unauthorized absence (UA) or in a deserter status must be reported to NCIS if the command believes that their absence will have an adverse effect on national security.

6. Personnel Out-Processing. Access to classified information terminates when an individual transfers from a command. Commands will debrief individuals, but execution of a security termination statement (STS) is not required because affiliation continues and clearance requirements will normally remain. Commands will administratively withdraw an individual's access when a permanent change in official duties eliminates the requirements for security clearance and access and when the individual separates or retires from the DON or otherwise terminates employment. The individual will be debriefed and will execute an STS which will be forwarded to HQMC Manpower Management Separation and Retirement (MMSR) for inclusion in the individual's service record or official personnel folder.

7. Visitor Control Procedures. Commanding officers will establish procedures to ensure that only visitors with an appropriate level of personnel security clearance and need to know are granted access to classified information. Those procedures shall include verification of clearance and eligibility through the JPAS. The visitor will sign in to a visitor logbook that the intelligence section maintains. The visitor logbook will maintain a record of visitors into their secure room and access to classified information. All visitors must be eligible and have been read-in to their appropriate clearance level before handling classified information.

a. Visit Requests. When a visit to 11th Marines will involve access to classified information, the security manager of the visitor will submit a visit request through the JPAS. The visit request will contain the requirements listed in reference (j), chapter 11.

b. Access Control. In the event that uncleared personnel require access to classified spaces (e.g. for the purposes of maintenance or facilities inspections, etc.), they will be accompanied at all times by appropriately cleared security personnel (i.e. security assistant(s)). Entrance to the

classified space in question will be announced by the escort prior to making entry, and will be succeeded by a period of time that is sufficient to allow personnel working in the classified space to sanitize monitors, cover hard-copy classified material, and cease any classified verbal conversations.

c. Foreign Officers. Although non-U.S. citizens are not eligible for security clearance, access to classified information may be justified for compelling reasons in furtherance of the DON mission, including special expertise. Limited Access Authorizations (LAAs) may be considered under the circumstances outline in reference (j), chapter 9. Procedures for visits by foreign nationals and representatives of foreign entities are outlined in reference (j), chapter 11. 11th Marines currently does not have any foreign liaison officers or foreign exchange officers. Additional questions regarding the disclosure of classified material to foreign nationals should be directed, via the security manager, to the 1st Marine Division, foreign disclosure officer at (760)763-9397.

8. Industrial Security Program. Due to minimal contractors contributing to the mission of 11th Marines, there is no need for a Contracting Officer's Representative for Security (CORS). The Command Security Manager will coordinate regularly with the IAM and the Contracting Agency Security Manager to ensure all security procedures are being followed to include IT designations, investigations, and eligibility requirements. For more information on Industrial Security Programs, see reference (e).

a. Key Personnel. Personnel that will maintain regular communication with each other to ensure the effectiveness of the 11th Marines Industrial Security Program include:

(1) Commanding Officer

(2) Security Manager

(3) Assistant Security Manager

(4) Contracting Agency Security Manager

(5) Individual Contractor

b. Procedures. Key procedures to ensure an effective Industrial Security Program include:

(1) The individual contractor must check in with the Security Manager and/or Assistant Security Manager to be properly vetted through JPAS.

(2) The Contracting Agency Security Manager must submit a visit request through JPAS for the duration of the contractor's stay.

(3) The Contracting Agency Security Manager must send the Command Security Manager the contractor's Statement of Work (SOW) and Department of Defense Contract Security Classification Specification Form (DD 254) to properly manage applicable security clearance eligibility and IT designation levels.

(4) The individual contractor must complete all required security training to utilize 11th Marines assets, including NIPR and SIPR systems. If the contractor has completed their required annual training with their contracting agency, they must provide the Command Security Manager with proof of completion.

(5) Once the individual contractor is no longer required to assist 11th Marines, they must check out of the unit with the Security Manager and/or Assistant Security Manager via JPAS and provide any necessary documentation pertaining to their work with 11th Marines, if applicable.