Headquarters, U.S.
Marine Corps

MCO P5510.18A
PCN 10208490600

UNITED STATES MARINE CORPS INFORMATION AND PERSONNEL SECURITY PROGRAM MANUAL (SHORT TITLE: MARINE CORPS IPSP)

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

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

MCO P5510.18A
ARS
3 Feb 00

MARINE CORPS ORDER P5510.18A W/CH 1

From: Commandant of the Marine Corps
To: Distribution List

Subj: UNITED STATES MARINE CORPS INFORMATION AND PERSONNEL SECURITY PROGRAM MANUAL (SHORT TITLE: MARINE CORPS IPSP)

Ref: (a) SECNAVINST 5510.36
(b) SECNAVINST 5510.30A
(c) DoD 5220.22-M
(d) DoD 5220.22-R
(e) OPNAVINST 5530.14B

Encl: (1) LOCATOR SHEET

1. Purpose. To establish the Information and Personnel Security Program (IPSP) within the United States Marine Corps.
2. Cancellation. MCO P5510.18, MCO 5521.3H.

3. Action

a. All Marine Corps commands and organizations will ensure compliance with the provisions of this Manual as it pertains to the Information and Personnel Security Program (IPSP). "Commanding officer" is used throughout this Manual as a generic term for the head of an organizational entity and includes commander, commanding general, director, officer in charge, etc. Responsibilities assigned to the commanding officer by this Manual may be delegated unless specifically prohibited.

b. The Commandant of the Marine Corps (CMC), Administration and Resource Management Division, Headquarters Administrative Security Branch (ARS) will conduct periodic reviews of security programs at Marine Corps commands.

4. Reporting Requirements. All reports and requests will be submitted to the Chief of Naval Operations (CNO) (N09N2), per the provisions of References (a) and (b), with a copy to CMC (ARS), unless otherwise indicated.

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

5. Recommendations, comments, and inquiries concerning this Manual are solicited and should be submitted to the CMC (ARS), telephone number Commercial (703) 614-2320/3609 or DSN 224-2320/3609.

6. Summary of Changes. SECNAVINST 5510.36 and SECNAVINST 5510.30a incorporate many changes from OPNAVINST 5510.1H. These instructions provide the basis for the Department of the Navy's Security Program, however, Marine Corps specific requirements necessitated more stringent application of security policies in several areas. This Manual consolidates these changes into one document, which should be used in conjunction with SECNAVINST 5510.36 and SECNAVINST 5510.30a. Changes in this Manual include:

a. Chapter 1. Establishes the Marine Corps IPSP and identifies CMC (ARS) as the Marine Corps' Information and Personnel security policy authority. This chapter also identifies phone numbers for CMC (ARS).

b. Chapter 2. Outlines commanding officer responsibilities along with the specific requirements for each member of the commands' security team.

c. Chapter 3. Outlines security education requirements and responsibilities.

d. Chapter 4. Provides specific Marine Corps related personnel security information.

e. Chapter 5. Provides Marine Corps specific guidance and policy for safeguarding classified information. Also includes guidance for information drawn from the SIPRNET.

7. Applicability. This Manual applies to all Marines and civilians assigned to Marine Corps commands.

8. Certification. Reviewed and approved this date.

LEO J. KELLY
By direction

DISTRIBUTION: PCN 10208490600

Copy to: 7000110 (55)
7000098 (4)
4090005/7230005/8145004, 005 (2)
3001001/700093, 144/7221001/8145001 (1)

«<--->»
Date signed: 06/25/2002 MARADMIN Number: 343/02 R 170001Z JUN 02
CMC WASHINGTON DC(n)
TO ML MARADMIN(n)
MARADMIN
INFO CNO WASHINGTON DC(n)
CNO WASHINGTON DC
UNCLAS
MARADMIN 343/02
MSGID/GENADMIN/CMC WASHINGTON DC ARS//
SUBJ/CHANGE 1 TO MCO P5510.18A//
REF/A/MCO/CMC/AMPN-/P5510.18A//
RMKS/1. AS SET FORTH IN MCO P5510.18A, THE MARINE CORPS IS CURRENTLY THE ONLY SERVICE WITHIN THE DEPARTMENT OF DEFENSE TO REQUIRE SPECIFIC ADMINISTRATIVE PROCEDURES FOR CONTROLLING GENSER SECRET MATERIAL; I.E., NATIONAL SECURITY INFORMATION UNDER THE PROVISIONS OF E.O. 12958 BUT NOT SUBJECT TO ENHANCED SECURITY PROTECTION REQUIRED FOR SPECIAL ACCESS PROGRAM INFORMATION.
2. THE PROLIFERATION OF GENSER SECRET COMPUTER NETWORKS, SUCH AS THE SIPRNET, HAS INCREASED ACCESS TO GENSER SECRET INFORMATION. THE EASE OF DISSEMINATION OF THAT INFORMATION HAS RENDERED THE CONTROLS MANDATED BY MCO P5510.18A IMPRACTICAL. MOREOVER, THE LEVELS OF OVERSIGHT AFFORDED BY THE INFORMATION SYSTEMS SECURITY MANAGER (ISSM) AND COMMAND OR AGENCY SECURITY MANAGER IN ACCORDANCE WITH THE COMMANDER'S SECURITY POLICY IS ADEQUATE AND SUFFICIENT TO SAFEGUARD GENSER SECRET MATERIAL.
3. TO ALIGN THE MARINE CORPS AND SECRETARY OF THE NAVY INFORMATION SECURITY PROCEDURES AND TO ENSURE ADEQUATE AND ENFORCEABLE MARINE CORPS INFORMATION SECURITY POLICY, REPLACE PARAGRAPH 5003 OF THE ORDER WITH THE FOLLOWING:
SECRET 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 REGULATION.
4. COMMANDERS AND THEIR SECURITY MANAGERS ARE REMINDED THAT THE LOSS OR COMPROMISE OF CLASSIFIED INFORMATION PRESENTS A THREAT TO NATIONAL SECURITY AND MUST BE PROPERLY INVESTIGATED IN ACCORDANCE WITH THE SECNAVINST 5510.36. THE ABOVE CHANGE DOES NOT DIMINISH THE CONTINUED REQUIREMENTS TO PROPERLY SAFEGUARD SECRET MATERIAL THROUGH APPROPRIATE REPRODUCTION, TRANSMISSION, STORAGE, MARKING AND DESTRUCTION PROCEDURES.
5. POC AT HQMC IS MAJ E. M. HENSEN AT (703) 614-2320/3609, DSN 224-XXX OR EMAIL AT HENSENEM@HQMC.USMC.MIL//

LOCATOR SHEET

Subj: UNITED STATES MARINE CORPS INFORMATION AND PERSONNEL SECURITY PROGRAM MANUAL (SHORT TITLE: MARINE CORPS IPSP)

Location: _____

(Indicate the location(s) of the copy(ies) of this Manual.)

ENCLOSURE (1)

MARINE CORPS IPSP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person

CONTENTS

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

1000. PURPOSE

1. This Manual establishes the Marine Corps Information and Personnel Security Program (IPSP). The IPSP applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission, and destruction of classified information. This Manual also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this Manual to identify any matter, document, product, or substance on or in which classified information is recorded or embedded.

2. This Manual implements the IPSP within the Marine Corps in compliance with the references and specific Marine Corps guidelines to establish an effective Marine Corps Security Program.

3. Applicability. This Manual applies to all personnel, military and civilian assigned to or employed by any element of the Marine Corps. Contracting officers must ensure compliance with contractors by properly coordinating with command security managers and the Defense Security Service prior to completion of contract negotiations. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), reference (c), is the reference for specific information with regard to contractors working with classified information. Commanding officers are responsible for compliance.

4. Scope. This Manual establishes the minimum standards for compliance with the IPSP for the United States Marine Corps.

1001. POLICY GUIDANCE

1. Assistance Via the Chain of Command. Marine Corps activities are required to obtain guidance or interpretation of policy and procedures in this Manual from CMC (ARS) via the operational chain of command. Telephone inquiries may be made to the CMC (ARS) at commercial (703) 614-2320/3609 or DSN 224-2320/3609. After-hours voice mail is available.

2. Combat Operations. Recognizing that combat can create special circumstances, conditions may dictate a modification to these guidelines. Commanding officers may modify the requirements of this Manual as necessary to meet local conditions during combat, combat-related, or contingency operations. Coordination must be effected with and between service, subordinate, and adjacent organizations to ensure agreement and must be effected prior to implementation. Additionally, modifications to storage requirements in a field environment must pay particular attention to the threat.

3. Waivers and Exceptions. Waivers to this Manual will be requested from the CNO (N09N2) via CMC (ARS). Submission requirements are outlined in SECNAVIST 5510.30A and SECNAVIST 5510.36. Waivers and exceptions are self-canceling at the end of the approved time, unless a renewal request is approved by the CNO (N09N2).

4. Alternative or Compensatory Security Control Measures. Commands desiring to implement alternative or compensatory security control measures must submit requests to the CNO (NO9N2) via CMC (ARS). Procedures for submitting requests and requirements for approval are stated in SECNAVINST 5510.36, chapter 7, paragraph 7-8.

1002. NATIONAL AUTHORITIES FOR SECURITY MATTERS. The CMCadministers the Marine Corps IPSP within the Marine Corps.
The Director of Administration and Resource Management (AR) has been designated to manage the IPSP for the Marine Corps:

a. CMC (ARS) is responsible for developing and implementing security related programs and policies Marine Corps-wide.

b. CMC (CIC) is responsible for implementation of Counterintelligence (CI) and human intelligence programs which protect the resources of the Joint Task Force (JTF)/Marine Air Ground Task Force (MAGTF) commander, DoD, and the U.S. intelligence community against espionage, sabotage, subversion, terrorism, assassinations or other intelligence actions conducted by or on behalf of foreign powers, organizations, or persons. These functions do not include personnel, physical, document, or communications security programs.

CHAPTER 2

COMMAND SECURITY MANAGEMENT

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. BASIC POLICY. Commanding officers are responsible for compliance with and implementation of the Marine Corps Information and Personnel Security Program (IPSP) within their command.

2001. COMMANDING OFFICER

1. An effective security program relies on a team of professionals working together to fulfill the commanding officer's responsibilities. Billet designations will be made in writing.

2. Commanding Officer's responsibilities:

a. Designate a security manager.

b. Designate a Top Secret Control Officer (TSCO), if the command handles Top Secret information.

c. Designate an Information Systems Security Manager (ISSM), if the command processes data in an automated system.

d. Designate a security officer to manage facilities security.

e. Designate a Special Security Officer (SSO) to administer the command Sensitive Compartmented Information (SCI) security program.

f. Issue a written command security instruction. See Appendix A.

g. An Industrial Security Program will be established in compliance with References (a),(b),(c), and (d).

h. 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.

i. Prepare an emergency plan for the protection of classified material. See Appendix B.

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

k. Ensure that the performance rating systems of all Marine Corps military and civilian personnel, whose duties significantly involve the creation, handling, or management of national security information (NSI), include a security element on which to be evaluated.

2002. SECURITY MANAGER

1. Every command in the Marine Corps eligible to receive classified information is required to designate a security manager in writing.

2. The security manager will be afforded direct access to the commanding officer to ensure effective management of the command's security program.

3. The command security manager may be assigned full-time, part-time, or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the previous 5 years.

4. The command security manager must be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc.

5. Commanding officers will obtain formal training for their security managers. The Navy Security Manager's Course is offered by the Naval Criminal Investigative Service (NCIS) Mobile Training Team (MTT). Information on the MTT and quotas to attend the course may be obtained by calling (757) 464-8925, DSN 680-8925. Commands may host the MTT with prior coordination with the team. Additional information may be found on the Navy Security website at CNO WEB URL http://www.navysecurity.navy.mil/.

2003. DUTIES OF THE SECURITY MANAGER

1. 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 duties described in this Manual may apply to a number of personnel. The security manager must be cognizant of command security functions and ensure the security program is coordinated and inclusive of all requirements. The security manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures, and must provide assistance in solving security problems. The security manager is key in developing and administering the command's Information and Personnel Security Program (IPSP).

2. The below listed duties apply to all security managers:

a. Serves as the commanding officer's advisor and direct representative in matters pertaining to the classification, safeguarding, transmission and destruction of classified information.

b. Serves 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.

c. Develops written command information and personnel security procedures, including an emergency plan which integrates emergency destruction plans where required.

d. Formulates and coordinates the command's security awareness and education program.

e. Ensures security control of visits to and from the command when the visitor requires, and is authorized, access to classified information.

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

g. Ensures that access to classified information is limited to those who are eligible and have the need to know.

h. Ensures that personnel security investigations, clearances and accesses are properly recorded.

i. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

j. Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

k. Coordinates with the command information systems security manager on matters of common concern.

l. Ensures that all personnel who have had access to classified information who are separating, retiring or relieved for cause per Reference (e) have completed a Security Termination Statement.

m. Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information. SF 312's will be forwarded to HQMC at the address listed in Reference (e).

2004. TOP SECRET CONTROL OFFICER (TSCO). Commands that handle Top Secret material will designate a TSCO in writing. The TSCO must be a Gunnery Sergeant (E-7) or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of an SSBI or SSBI/PR completed within the previous 5 years.

2005. SECURITY ASSISTANTS

1. Commanding officers may elect to assign assistant security personnel depending on the size of the command, mission and particular circumstances. Assistants may include the following positions or others, depending on command requirements.

2. Assistant Security Manager. Persons designated as assistant security managers must be U.S. citizens, and either Staff Sergeant (E-6) or above, or civilians GS-6 or above. The designation must be in writing. Assistant security managers must have an SSBI if they are designated to issue interim security clearances; otherwise, the investigative and clearance requirements will be determined by the level of access to classified information required.

3. Security Assistant. Civilian and military member employees performing administrative functions under the direction of the 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.

4. Top Secret Control Assistant (TSCA). Individuals may be assigned to assist the TSCO as needed. The designation will be in writing. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian

employee GS-5 or above. An established Top Secret security clearance eligibility is required. Top Secret couriers are not considered to be Top Secret control assistants.

2006. CONTRACTING OFFICER'S REPRESENTATIVE (COR). Commands that award classified contracts to industry will appoint, in writing, one or more qualified security specialists as the Contracting Officer's Representative (COR). The COR is responsible to the security manager for coordinating with program managers and technical and procurement officials. The COR will ensure that the industrial security functions are accomplished when classified information is provided to industry for performance on a classified contract.

2007. INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

1. 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.

2. The ISSM is responsible to the commanding officer for development, maintenance, and implementation of the 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 Navy INFOSEC web site at http://infosec.nosc.mil/content.html provides further guidance.

2008. SPECIAL SECURITY OFFICER (SSO)

1. Commands in the DON accredited for and authorized to receive, process and store SCI will designate an SSO. The SSO is the principal advisor on the SCI security program in the command and is responsible to the commanding officer for the management and administration of the program. The SSO will be afforded direct access to the commanding officer to ensure effective management of the command's SCI security program. The SSO will be responsible for the operation of the Sensitive Compartmented Information Facility (SCIF) and the security control and use of the SCIF. All SCI matters are referred to the SSO.

2. The security manager cannot function as the SSO unless authorized by the Director, Office of Naval Intelligence (ONI) or Commander, Naval Security Group (COMNAVSECGRU).

3. Although the SSO administers the SCI program independent of the security manager, the security manager must account for all clearance and access determinations made on members of the command. There is great need for cooperation and coordination between the SSO and security manager, especially for personnel security matters. The security manager and the SSO must keep each other advised of any changes in status regarding clearances and command security program policies and procedures as they may impact on the overall command security posture.

2009. INSPECTIONS, ASSIST VISITS, AND REVIEWS

1. Commanding officers are responsible for evaluating the security posture of their subordinate commands.

2. Commanding officers will conduct inspections, assist visits, and reviews to examine overall security posture of subordinate commands. Inspections will be conducted annually.

3. A command information and personnel security program self-inspection guide is provided in references (d) and (e). These checklists may be modified to meet local command needs. The IGMC Security Inspection checklist may be found in the Automated Inspection Reporting System (AIRS).

2010. SECURITY SERVICING AGREEMENTS (SSA)

1. Commands may perform specified security functions for other commands via security servicing agreements. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including;

a. A command provides security services for another command, or the command provides services for a tenant activity;

b. A command is located on the premises of another Government entity and the host command negotiates an agreement for the host to perform security functions;

c. A senior in the chain of command performs or delegates certain security functions of one or more subordinate commands;

d. A command with particular capability for performing a security function agrees to perform the function for another.

e. A command is established expressly to provide centralized service (for example, Personnel Support Activity or Human Resources Office).

f. When either a cleared contractor facility or a long-term visitor group is physically located on a Navy or Marine Corps installation.

2. A security servicing agreement will be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement will include requirements for advising commanding officers of any matters which may directly affect the security posture of the command. Append security servicing agreements to the command security instruction.

2011. STANDARD PROGRAM REQUIREMENTS. Each command which handles classified information is required to prepare and keep current a written command security instruction, specifying how security procedures and requirements will be accomplished in the command. Appendix A applies.

2012. PLANNING FOR EMERGENCIES. Commands will establish a plan for the protection and removal of classified National Security Information (NSI) under its control during emergencies. Depending upon the location of the command, the plan may direct destruction of classified NSI in an emergency. The plan should be made part of the overall disaster preparedness plan of the command security program instruction. Appendix B applies.

CHAPTER 3

SECURITY EDUCATION

CHAPTER 3

SECURITY EDUCATION

3000. BASIC POLICY

1. Each command will establish and maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures.

2. The purpose of the 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.

3001. RESPONSIBILITY

1. CMC (ARS) is responsible for policy guidance, education requirements and support for the Marine Corps security education program. Development of security education materials for use throughout the Marine Corps must be coordinated with CMC (ARS) for consistency with current policies and procedures.

2. Recruit depots are responsible for indoctrinating military personnel with a basic understanding and definition of classified information and why and how it is protected. Civilian employees and contractor personnel employed by the Marine Corps for the first time must also be given a basic security indoctrination by the employing activity if they will handle classified material.

3. Commanding officers are responsible for security education in their commands, ensuring time is dedicated for training and awareness. Personnel in positions of authority, in coordination with the command security manager, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand the security requirements for their particular assignment. Continual training is an essential part of command security education and leaders/supervisors must ensure that such training is provided.

3002. SCOPE. The scope for security education is outlined in SECNAVINST 5510.30A.

3003. MINIMUM REQUIREMENTS. Minimum security education requirements are outlined in SECNAVINST 5510.36, Chapter 4.

CHAPTER 4

PERSONNEL SECURITY INVESTIGATIONS

4000. BASIC POLICY

1. 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 their loyalty, reliability, and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations.

2. Only the following officials are authorized to request PSI's on individuals under their jurisdiction:

a. Commanding officers and OIC's of organizations and activities.

b. Director, Department of the Navy Central Adjudication Facility (DON CAF); and

c. Commanding General, Marine Corps Recruiting Command (CG MCRC).

3. The scope of the investigation conducted will be commensurate with the level of sensitivity of the access required or position occupied. Only the minimum investigation to satisfy a requirement may be requested.

4. The DON CAF will assign clearance eligibility at the highest level supportable by the investigation completed. Access granted is a local command responsibility and is based on need to know established by the commander, not the individual requesting access. Access must not be granted automatically and does not have to be granted at the level of eligibility.

5. The Defense Security Service (DSS) or, where specified, the U.S. Investigative Service (USIS), conducts (or controls the conduct of) all PSI's for the Marine Corps. Marine Corps elements are prohibited from conducting PSI's, including local public agency inquiries, unless specifically requested to do so by an authorized investigative agency (e.g., DSS or USIS). An exception to this restriction is made for Marine Corps overseas commands employing foreign nationals for duties not requiring access to classified material. secnavinst 5510.30a, paragraph 6-8, subparagraph (n) provides further details.

6. Per secnavinst 5510.30a, PSI's and Periodic Reinvestigations (PR) will not be requested for any civilian or military personnel who will be retired, resigned, or separated with less than 1 year service remaining. Fiscal restraints and overburdened investigative agencies prevent the submission of all but essential requests for investigation. Exceptions will be granted only for those personnel whose participation in a Special Access Program is documented with appropriate orders and whose assignment is contingent upon completion of the required PR.

7. Validation of current security clearance status is required prior to awarding access to classified national security information and must be determined prior to submitting a PSI. The Marine Corps Total Force System (MCTFS) provides accurate and updated information and may be used to make this determination. If MCTFS is not available or if the person in question is a civilian Marine, the following options are available to make an accurate determination:

a. Consult the Defense Clearance and Investigations Index (DCII) database. This information is sufficient to award access at the level of clearance eligibility specified in the database. Secnavinst 5510.30a provides specific guidance on requesting access to the DCII.

b. Submit a Personnel Security Action Request, OPNAV Form 5510/413 to DONCAF requesting a status on the person's clearance eligibility.

8. When a Marine PCS's or a civilian transfers within the DON, the only action required is a termination of access at the losing command. No action is required regarding clearance eligibility. SECNAVINST 5510.30A provides specific guidance relating to actions upon termination of service.

9. SECNAVINST 5510.30A, par 6-16 (8) guidance regarding Marine Corps tracer action via MCTFS is invalid. Tracer action, using the guidance for tracer timelines, must be requested from DON CAF with a 5510/413. These requests should be faxed to (202) 433-8875/8899, DSN 288-8875/8899.

10. The Deputy Secretary of Defense determined that additional measures were warranted to increase the awareness of individuals who were entrusted with access to Top Secret information and/or indoctrinated into Special Access Programs. In compliance, the statement below will be read aloud and 'attested to', in the presence of a witness other than the person administering the brief. This attestation is not a legally binding oath and will

not be sworn to. Attestation administration is required only one time, usually when the original SF 312, Classified Information Nondisclosure Agreement or 1879-1, Sensitive Compartmented Information Nondisclosure agreement is signed. Commands are encouraged, however, to implement the attestation statement as a part of the command's annual security refresher training and apply it to all levels of clearance eligibility. No documentation or reporting is required; however, inspection visits may inquire into the procedures in place to implement this guidance.

Attestation Statement:

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official need to know. I further understand that, in being granted access to classified information and/or SCI/SAP, a special confidence and trust has been placed in me by the United States Government.

CHAPTER 5

SAFEGUARDING

CHAPTER 5

SAFEGUARDING

5000. BASIC POLICY

1. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited Automated Information Systems (AIS), 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 may be designated, in writing, by the commanding officer as restricted areas per OPNAVINST 5530.14B. Decisions regarding designations of restricted areas, their levels, and criteria for access are at the discretion of the commanding officer. All personnel shall comply with the need-to-know policy for access to classified information.

2. Classified information is the property of the U.S. Government and not personal property. Military or civilian personnel who resign, retire, separate from the DON, or are released from active duty, shall return all classified information in their possession to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers.

5001. APPLICABILITY OF CONTROL MEASURES. Classified information shall be afforded a level of control commensurate with its assigned security classification level. This policy encompasses all classified information regardless of media.

5002. TOP SECRET CONTROL MEASURES

1. All Top Secret information (including copies) originated or received by a command shall be continuously accounted for, individually serialized, and entered into a command Top Secret log. The log shall completely identify the information, and at a minimum, include the date originated or received, individual serial numbers, copy number, title, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken.

2. In addition to the marking requirements of chapter 6 of SECNAVINST 5510.36, Top Secret information originated by the command shall be marked with an individual copy number in the following manner "Copy No.__ of __ copies." Exceptions to this rule are allowed for publications containing a distribution list by copy number and for mass-produced reproductions when copy numbering would be cost prohibitive. In the latter case, adequate and readily available documentation shall be maintained indicating the total copies produced and the recipients of the copies.

3. TSCO's shall obtain a record of receipt (typically a classified material receipt) from each recipient for Top Secret information distributed internally and externally.

4. Top Secret information shall be physically sighted or accounted for at least annually, and more frequently as circumstances warrant (e.g., at the change of command, change of TSCO, or upon report of loss or compromise). As an exception, repositories, libraries or activities which store large volumes of classified material may limit their annual inventory to all documents and material to which access has been given in the past 12 months, and 10 percent of the remaining inventory. See SECNAVINST 5510.36, chapter 2, paragraph 2-3 for TSCO duties.

5003. SECRET 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 regulation.

5004. CONFIDENTIAL CONTROL MEASURES. Procedures for protection of Confidential information are less stringent than those for Secret; only one witness is required for destruction. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. Administrative provisions are required, however, to protect Confidential information from unauthorized disclosure by access control and compliance with the regulations on marking, storage, transmission, and destruction.

5005. WORKING PAPERS

1. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents. Working papers shall be:

a. Dated when created;

b. Conspicuously marked "Working Papers" on the first page in letters larger than the text;

c. Marked centered top and bottom on each page with the highest overall classification level of any information they contain;

d. Protected per the assigned classification level; and

e. Destroyed, by authorized means, when no longer needed.

2. Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

5006. TOP SECRET MESSAGES

1. Top secret messages, including top secret "Special Handling" messages, SPECAT, and "Personal For" messages are received at the Communications Center. A Top Secret Disclosure Sheet will be attached to the message and forwarded to the command TSCO with distribution instructions. The Top Secret Disclosure Sheet will be signed by each individual who processes or takes possession of the message. After initial distribution has been made, only the command TSCO may authorize reproduction of top secret messages. Top Secret messages are on temporary loan to the user and will be returned to the command TSCO for disposition when no longer needed.

2. When messages of an urgent nature are received requiring an immediate response, the recipient and TSCO will both be notified promptly so that necessary action can be taken to answer the requirements of the message and simultaneously bring the message under control.

5007. SECRET MESSAGES Distribution of Secret messages, excluding special handling messages, may be made directly to the appropriate command and/or staff agencies. Because of the large volume of secret messages, decentralized accounting procedures are authorized for secret message traffic. These messages will be afforded the same level of protection against compromise as standard secret documents. Secret messages should be treated as working papers.

5008. REPRODUCTION

1. The proliferation of reproduction machines throughout the Marine Corps has compounded the problems associated with reproducing classified material. The convenience of reproduction equipment does not preclude obtaining the proper authorization needed for reproducing classified material.

2. Top Secret information will not be reproduced without the consent of the originating activity, higher authority, and the command's Top Secret Control Officer.

3. Commanding officers must designate officials who will approve all requests to reproduce Top Secret and Secret material. These officials in turn have the responsibility to ensure that all reproduction prohibitions are observed and that the reproduction of classified material is kept to an absolute minimum. Personnel must be made aware of the requirement for approval by one of these designated officials before reproducing classified material. Where possible, two people will be involved in reproducing classified material to ensure positive control and safeguarding of reproduced material.

4. Records will be maintained for a period of 2 years to show the number and distribution of all reproductions of Top Secret documents, classified documents covered by special access programs distributed outside the originating agency, and Secret and Confidential documents marked with special dissemination and reproduction limitations.

5. To the extent possible, controlled areas for reproduction will be established. At a minimum, the reproduction equipment authorized for reproducing classified material will be specifically designated and signs will be prominently displayed on or near the equipment to advise users. A sign may read, for example, "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY (designated official)." Machines that are not authorized for the reproduction of classified material will be posted with a warning notice such as "THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL." Reproduction machines will be located in areas that are easily observable to ensure that only authorized copies are being made and the number of copies is kept to a minimum.

6. If the designated equipment involves reproduction processes using extremely sensitive reproduction paper, the paper will be used and stored in a manner to preclude image transfer of classified information.

7. Reproduced copies of classified documents will be afforded the same security controls as those required for the original documents.

8. Reproduced material must show the classification and other special markings which appear on the original material from which copied. All reproduced material will be double checked and remarked when the markings are not clear.

9. Any samples, waste, or overruns resulting from the reproduction process, will be safeguarded according to the classification of the information involved. This material will be promptly destroyed as classified waste. Areas surrounding reproduction equipment will be checked for classified material that may have been left on nearby desks or thrown in waste-baskets. In the event the machine malfunctions, it will be checked to ensure that all copies have been removed. After reproducing classified material, the machine will be checked to ensure the original and all copies have been removed.

5009. CLASSIFIED ELECTRONICALLY TRANSMITTED MATERIAL

1. Classified information obtained from classified computer systems such as the SIPERNET must be reviewed to determine proper classification to prevent inadvertent compromise. While some information available via classified networks may be unclassified, the assumption must not be made that the entire document is unclassified.

2. If information drawn from classified networks is not marked, either through document or portion markings contact the document's originator to determine the classification of the material.

3. If a classified document is received via electronic means and printed, the printed document will be handled and controlled commensurate with the highest level of classification in the document.

APPENDIX A

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. The security manager shall assess the vulnerability of the command's classified information to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified information, mission of the command, countermeasures available and the cost and effectiveness of alternative courses of action. Results of this assessment shall be used to develop a command security instruction which will mirror the organization of this regulation and identify any unique command requirements. The command security instruction shall supplement this regulation and other directives from authorities in the command administrative and operational chain.

2. Incorporate the following into the command security instruction:

a. The purpose, applicability, and relationship to other directives, particularly this regulation.

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Cite and append SSA's, if applicable.

e. Describe procedures for internal and subordinate security reviews and inspections.

f. Specify internal procedures for reporting and investigating loss, compromise, and other Security discrepancies.

g. Establish procedures to report CI matters to the nearest NCIS office.

h. Develop an IPSP security education program. Assign responsibilities for briefings and debriefings.

i. State whether the commanding officer and any other command officials have been delegated Top Secret or Secret original classification authority.

j. Establish procedures for the review of classified information prepared in the command to ensure correct classification and marking. Identify the sources of security

classification guidance commonly used, and where they are located.

k. Develop an industrial security program and identify key personnel, such as the Contacting Officer's Representative, if applicable.

l. Specify command responsibilities and controls on any special types of classified and controlled unclassified information.

m. Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.

n. Identify requirements for the safeguarding of classified information to include how classified information shall be protected during working hours; stored when not in use; escorted or hand carried in and out of the command; and protected while in a travel status. Other elements of command security which may be included are key and lock control; safe and door combination changes; location of records of security container combinations; procedures for emergency access to locked security containers; protecting telephone conversations; conducting classified meetings; the safeguarding of U.S. classified information located in foreign countries; AIS processing equipment; and residential storage arrangements.

o. Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command emergency destruction plan, as a supplement, when required.

p. Establish command visitor control procedures to accommodate visits to the command involving access to, or disclosure of, classified information. Identify procedures to include verification of personnel security clearances and need-to-know.

APPENDIX B

EMERGENCY PLAN AND EMERGENCY DESTRUCTION SUPPLEMENT

PART ONE: EMERGENCY PLAN

1. Commanding officers shall develop an emergency plan for the protection of classified information in case of a natural disaster or civil disturbance. This plan may be prepared in conjunction with the command's disaster preparedness plan.

2. Emergency plans provide for the protection of classified information in a way that will minimize the risk of personal ijury or loss of life. For instance, plans should call for immediate personnel evacuation in the case of a fire, and not require that all classified information be properly stored prior to evacuation. A perimeter guard or controlling access to the area will provide sufficient protection without endangering personnel.

3. In developing an emergency plan, assess the command's risk posture. Consider the size and composition of the command; the amount of classified information held; situations which could result in the loss or compromise of classified information; the existing physical security measures; the location of the command and degree of control the commanding officer exercises over security (e.g., a ship versus a leased private building); and local conditions which could erupt into emergency situations.

4. Once a command's risk posture has been assessed, it can be used to develop an emergency plan which can take advantage of a command's security strengths and better compensate for security weaknesses. At a minimum, the emergency plan shall designate persons authorized to decide that an emergency situation exists and to implement emergency plans; determine the most effective use of security personnel and equipment; coordinate with local civilian law enforcement agencies and other nearby military commands for support; consider transferring classified information to more secure storage areas in the command; designate alternative safe storage areas outside the command; identify evacuation routes and destinations; arrange for packaging supplies and moving equipment; educate command personnel in emergency procedures; give security personnel and augmenting forces additional instruction on the emergency plan; establish procedures for prompt notification of appropriate authorities in the chain of command; and establish the requirement to assess the integrity of the classified information after the emergency.

PART TWO: EMERGENCY DESTRUCTION SUPPLEMENT

1. Commands located outside the U.S. and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans (CMS-1A provides additional emergency destruction policy and guidance for commands that handle COMSEC information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of incidents or emergency destruction of classified information shall be reported to the CNO (N09N2).

2. The priorities for emergency destruction are: Priority One--Top Secret information, Priority Two--Secret information, and Priority Three--Confidential information.

3. For effective emergency destruction planning, limit the amount of classified information held at the command and if possible store less frequently used classified information at a more secure command. Consideration shall be given to the transfer of the information to AIS media, which will reduce the volume needed to be transferred or destroyed. Should emergency destruction be required, any reasonable means of ensuring that classified information cannot be reconstructed is authorized.

4. An emergency destruction supplement shall be practical and consider the volume, level, and sensitivity of the classified information held at the command; the degree of defense the command and readily available supporting forces can provide; and proximity to hostile or potentially hostile countries and environments. More specifically, the emergency destruction supplement shall delineate the procedures, methods (e.g., document shredders or weighted bags), and location of destruction; indicate the location of classified information and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified information.

5. Marine Corps commands and organizations aboard Naval vessels will ensure that they became familiar with the emergency destruction procedures in place aboard ship. Coordination must be effected to include Marine Corps classified material in the destruction plan.

APPENDIX C

COMMANDER'S CHECKLIST FOR VALIDATING ACCESS ELIGIBILITY

These instructions were developed to assist the commander in ensuring that only those personnel who are properly cleared possess access to classified information within the commend. Any questions arising which are not covered by these instructions may be answered with a review of SECNAVINST 5510.30A.

a. Determine the level of access required by the Marine/civilian.

b. Determine clearance eligibility by viewing the Marine Corps Total Force System (MCTFS) Basic Training Record or the Defense Clearance Investigation Index (DCII).

c. If Marine/civilian possesses appropriate eligibility, ensure the following:

(1) Confirm U.S. citizenship.

(2) Review Marine's service record book (SRB)/officer qualification record (OQR) and health/dental records for any derogatory information which would adversely affect eligibility.

(3) Assign access no higher than established eligibility and 'need to know' based solely on billet requirements.

(4) Record Marine on unit access roster.

d. If Marine/civilian does not possess appropriate eligibility, ensure the following:

(1) Confirm U.S. citizenship.

(2) Review Marine's SRB/OQR and health/dental record for any derogatory information which would adversely affect eligibility.

(3) Review SECNAVINST 5510.30A to determine investigative requirement.

(4) Submit request for appropriate investigation.

(5) Assign interim clearance per the provisions of SECNAVINST 5510.30A, par. 8-5.

(6) Assign access (less SCI) based on the level of interim clearance authorized and the 'need to know' based on billet requirements.

(7) Record Marine on unit access roster.