UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION
MARINE CORPS BASE QUANTICO
3250 CATLIN AVENUE
QUANTICO, VIRGINIA 22134 5001

MCINCR-MCBQO 5510.1E
B 054
FEB 13 2024

MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION-MARINE CORPS BASE QUANTICO ORDER 5510.1E

From: Commander, Marine Corps Installations National Capital Region-Marine Corps Base Quantico
To: Distribution List

Subj: UNITED STATES MARINE CORPS INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) DoD Manual 5200.01 (Vol I-III)
(b) SECNAV 5510.30C
(c) SECNAV 5510.36B
(d) MCO 5510.18B
(e) DoD Instruction 5200.48

1. Situation. This Order establishes the Marine Corps Installation National Capital Region-Marine Corps Base Quantico (MCINCR-MCBQ) Information and Personnel Security Program (IPSP) under the authority of references (a) through (c) and in compliance with reference (d).

2. Cancellation. MCINCR-MCBQO 5510.1D w/ch 1.

3. Mission. All commands and organizations within the purview of MCINCR-MCBQ shall ensure compliance and implement the provisions of this Order to protect classified information and ensure personnel are properly vetted to handle such information.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Apply uniform, consistent, and cost-effective policies and procedures for the classification, safeguarding, transmission and destruction of classified National Security Information; authorized 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 them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security.

(2) Concept of Operations. Commanding Officers implement IPSP(s) within internal and external elements throughout the MCINCR-MCBQ.

5. Administration and Logistics.

a. This Order is to reflect and enforce reference (d) aboard MCINCR-MCBQ for the IPSP.

b. Previous Order did not contain controlled unclassified information and was originally written within the 9 year timeline which has been changed to a 6 year requirement.

6. Command and Signal

a. Command. This Order is applicable to the MCINCR-MCBQ.

b. Signal. This Order is effective the date signed.

MICHAEL L. BROOKS

DISTRIBUTION: A

TABLE OF CONTENTS

Chapter 1

Introduction

1. Purpose. The Marine Corps IPSP is established to implement standards and procedures as required by references (a) through (c) and in accordance with reference (d) to:

a. Apply uniform, consistent, and cost-effective policies and procedures for the classification, safeguarding, transmission and destruction of classified National Security Information (NSI).

b. 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 them with classified NSI or assigning them to sensitive duties is clearly consistent with the interests of national security.

2. Applicability. This Order applies to all personnel (e.g., Marines, Navy personnel assigned/attached to Marine Corps Installation National Capital Region, Marine Corps Base Quantico, and includes government civilian employees, contractors and consultants) employed by, and/or working in any element aboard Marine Corps Base Quantico.

a. Contracting Officers shall ensure compliance with applicable policy by properly coordinating with Command Security Managers, Contracting Officer Security Representatives, and the Defense Security Service prior to completion of contract negotiations in which provisions for access to classified NSI is required.

b. Chapter 6 of this Order refers more readily to MCO 5510.18B which provides specific information concerning contractors working with classified NSI.

3. Scope. This Order establishes the minimum standards for the Marine Corps IPSP.

a. Commanding Officers are responsible for compliance with this Order.

b. This Order provides guidance on command security management, security education, information security, personnel security, industrial security, and North Atlantic Treaty Organization (NATO) information security.

c. The term classified NSI is generically used throughout this Order to identify any matter, document, product, substance, or item of equipment, on or in which classified NSI is recorded or embedded.

4. Assistance Via the Chain of Command

a. Marine Corps activities are required to obtain collateral related guidance or interpretation of policy and procedures in this Order from the security office via the operational chain of command.

b. Marine Corps activities are required to obtain sensitive compartmentalized information (SCI) security program related guidance or interpretation of policy and procedures in this Order from Marine Corps Intelligence Activity (MCIA) Special Security Officer (SSO) via the

operational chain of command. Telephone inquiries may be made to MCIA SSO (703) 693-6005.

5. Alternative Compensatory Control Measures (ACCM). Commanding Officers desiring to implement ACCM must submit requests to Deputy Under Secretary of the Navy, via HQMC Security Division (PS). Procedures for submitting requests and requirements for approval are outlined in reference (a).

6. Position Sensitivity Designation (PSD). Military positions are, by default, considered to be sensitive. This designation is supported by the investigative requirement of a NACLC/T3 for enlistment/appointment suitability.

a. The favorable adjudication of the NACLC/T3, with the assignment of secret eligibility, does not automatically grant access to classified NSI. However, it does make the individual eligible for information technology (IT) Level II privileges.

(1) A favorable determination suggests a level of reliability and trustworthiness commensurate with access to sensitive information or assignment to a sensitive position.

(2) If a military member is not eligible for access to classified NSI, the individual's Commander may not assign the individual to sensitive duties or allow access to sensitive information and sensitive IT systems.

b. Government civilian positions require a determination at the time of Position Description (PD) creation or revision concerning PSD(s). The sensitivity level assigned to the PD shall determine which investigation is authorized for submission for the individual. PSD(s) must be made in consultation with local Human Resource (HR) offices, the employing office, and the Command Security Manager.

c. Many civilian positions are sensitive at some level and shall require an investigation that will result in the assignment of clearance eligibility whether access to classified NSI is required. Reference (b) outlines the investigative requirement for each PSD.

(1) Those positions designated "non-sensitive" (no classified and no sensitive information access) require a Tier 1 (or equivalent level investigation). The **Questionnaire for Non-Sensitive Positions Standard Form 85 Revised December 2013** is used to conduct these investigations.

(2) Those positions requiring access to Secret, non-critical sensitive information, or IT II computer privileges require a Tier 3 (or equivalent level investigation). The **Questionnaire for National Security Positions Standard Form 86 Revised December 2010** is used to conduct these investigations.

(3) Those positions which require access to Top Secret information, designated critical-sensitive, special-sensitive, and/or IT Level I, require a Tier 5 (or equivalent level investigation).

(a) The **Questionnaire for National Security Positions Standard Form 86 Revised December 2010** is used to conduct these investigations.

(b) The Billet Identification Code must be coded with a "T" or "I".

7. Use of Social Security Number (SSN). Use of the full SSN will be consistent with the requirements of reference (d) and avoided wherever possible.

a. However, if use of the SSN becomes necessary, utmost care must be exercised in handling this information due to the sensitivity of the SSN.

b. If the individual does not possess documentation containing his/her Department of Defense (DoD) ID Number or SSN, either may be provided verbally or in writing, in a manner designed to prevent access by others. When using this method, data contained on the provided documentation must match Personal Identifiable Information (PII) on the Subject Summary Screen in Defense Information System for Security (DISS).

(1) If requesting PII for identification purposes only (and not entering the information into a system or form) a Privacy Act Advisory (PAA) must be provided.

(2) A PAA is like a Privacy Act Statement (PAS). It provides the authority and purpose for requesting the SSN and whether providing the SSN is voluntary or mandatory.

c. Use of the SSN is guided by the Privacy Act of 1974, as amended. Each request for an individual's SSN must be accompanied by a copy of the PAS.

8. Command Echelon

a. The Marine Corps does not typically use the term, "echelon of command" when describing degree of authority for program responsibility. However, reference (d) uses this descriptive term to delegate various authorities within this program and therefore additional guidance is warranted in this Order.

b. For clarification purposes, HQMC is the only "Echelon 1" command within the Marine Corps.

c. All Marine Forces (MARFOR) level commands and separate commands which report directly to HQMC are "Echelon 2" commands with all the authorities established in the references. All organizations shall follow the chain of command.

Chapter 2

Command Security Management

1. Basic Policy. Commanding Officers are responsible for compliance with and implementation of the Marine Corps IPSP or applicable SCI security program within their command. The effectiveness of the command's IPSP and SCI security program depends on the importance given by the Commanding Officer.

2. Commanding Officer Responsibilities. An effective IPSP relies on a team of professionals working together to fulfill the Commanding Officer's responsibilities.

a. Command security management responsibilities include:

(1) Designate a Command Security Manager in writing.

(2) Designate a Top-Secret Control Officer in writing if the command handles Top Secret information.

(3) Designate an Information System Security Manager in writing if the command processes data in an automated system.

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

(5) Designate a SSO in writing to administer the command SCI security program.

(6) Issue a written command security instruction based on your commands security footprint in support of your commander.

(7) Establish and maintain a self-inspection program. The self-inspection program must include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command and its subordinate command's IPSP. Reference (d) provides detailed instructions.

(8) Establish an industrial security program when the command engages in classified procurement or when cleared contractors operate within the areas under the Commanding Officer's control.

(9) Ensure that the Command 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.

(10) Prepare an Emergency Action Plan (EAP) for the protection of classified material.

(11) Ensure the command security inspections, program reviews, and assist visits are conducted for effectiveness of the IPSP in subordinate commands.

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

(13) Ensure implementation and required use of DISS.

(14) Ensure implementation of the DoD Continuous Evaluation Program (CEP).

b. Consideration must be given to continuation of program management responsibilities during deployments for operations and exercises.

(1) Billets occupied by civilian employees must be reviewed in relation to PD and deployment requirements.

(2) Remain Behind Elements must have an Individual designated as the Command Security Manager and, as appropriate, ensure that a Security Servicing Agreement (SSA) has been created for security services.

3. Command Security Manager. Commands in the Marine Corps eligible to receive classified NSI (e.g., all Squadron/Battalion level commands and above), are required to designate, in writing, a Command Security Manager per references (b) and (d).

a. All Command Security Manager appointment letters shall be uploaded to the HQMC PS site at: https://ehqmc.usmc.mil/org/ hqmcppo/PS/PSS/Blog/default.aspx. Click on the link, "Security Manager Appointment Letters" and the click on "Add a Document."

b. On occasion, separate commands below the Squadron/ Battalion level may also require a Command Security Manager depending on the mission and support available from parent commands.

c. A unit's choice to divest itself of current classified holdings is not sufficient to negate this requirement.

d. Due to the technical nature of the IPSP and applicable SCI security program, and the intricacies involved with program management for the programs, the Command Security Manager and SSO should be assigned as a primary, full-time duty at every available opportunity.

e. The Command Security Manager shall be a special staff officer and afforded direct access to the Commanding Officer to ensure effective management of the command's IPSP. Reference (d) requires the Command Security Manager and SSO to report directly to the Chief of Staff or Executive Officer (XO).

f. The presence of a Command Security Manager goes well beyond the management of classified NSI/material. They administer the Personnel Security Program, the Insider Threat Program, and manage Controlled Unclassified Information (CUI). The Command Security Manager supports PII protection when applied to other command applications (e.g., HR, Comptroller, Law Enforcement).

g. The Command Security Manager must be a military officer or civilian employee in the grade of GS-11 or above, with sufficient authority and staff to manage the IPSP for the command.

h. The Command Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated T5 or equal level investigation completed within the five years prior to assignment.

i. Though typically assigned as a collateral duty to XOs in operational commands, this duty may be assigned to any other officer in the command provided he or she can devote the necessary time and effort to effectively comply with all program requirements.

j. Commanding Officers shall allow for the formal training of security managers and assistant security managers within 180 days of appointment. Training requirements are described in Chapter 3 of this Order.

k. Each command shall prepare and maintain a written command security instruction, specifying how security procedures and requirements shall be accomplished in the command.

4. Duties of the Command Security Manager

a. The duties of the Command Security Manager are delineated in references (a) and (d). The Command Security Manager is the principal advisor to the Commanding Officer on the IPSP and is responsible to the Commanding Officer for the management of the program.

(1) The duties described in this Order may apply to several personnel.

(2) The Command Security Manager must be cognizant of command security functions and the command's mission to ensure the security program is coordinated and inclusive of all requirements.

(3) The Command Security Manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures and must help in solving security problems.

(4) The Command Security Manager plays a critical role in developing and administering the command's IPSP.
own

b. The duties listed below apply to all Command Security Managers:

(1) Serves as the Commanding Officer's advisor and direct representative in matters pertaining to the classification, safeguarding, transmission and destruction of classified NSI and CUI.

(2) Serves as the Commanding Officer's advisor and direct representative in matters regarding the eligibility of personnel to access classified NSI and assignment to sensitive duties.

(3) Develops written command IPSP procedures, including an EAP which integrates emergency destruction plans, where required.

(4) Develops an annually updated turnover binder to ensure continuity of the command's security program.

(5) Formulates and coordinates the command's security awareness and education program.

(6) Ensures security control of visits to and from the command when the visitor requires, and is authorized, access to classified NSI.

(7) Ensures that all personnel who shall handle classified NSI or shall be assigned to sensitive duties are appropriately cleared through coordination with the Department of Defense Central Adjudication Facility and that requests for personnel security investigations are properly prepared, submitted and monitored.

(8) Ensures that access to classified NSI is limited to those who are eligible and have a verifiable Need-to-Know.

(9) Ensures that Personnel Security Investigation (PSI), eligibility, and accesses are properly recorded within DISS.

(10) Coordinates the command CEP.

(11) Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

(12) Coordinates with the command ISSM on matters of common concern.

(13) Coordinates with the local Naval Criminal Investigative Service (NCIS) field office to ensure a steady flow of information related to the Marine Corps Insider Threat Program and the CEP.

(14) Ensures that all personnel who have had access to classified NSI who are separating, retiring, or whose access has been suspended for cause per references (b) and (d), have completed a Security Termination Statement (STS).

(a) For military personnel, all completed STS must be forwarded to HQMC Manpower and Reserve Affairs (M&RA) (MMRP20) for inclusion in the Official Military Personnel File.

(b) For civilian personnel, all completed STS must be forwarded to the appropriate servicing HR office.

(15) Ensures all personnel execute a **CLASSIFIED NATIONAL SECURITY INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312** prior to granting initial access to classified NSI. A hard copy shall be forwarded to HQMC M&RA (MMRP-20) for Marines and to the servicing civilian HR office for civilian employees, with the execution documented within DISS.

(16) Periodically instruct members of the command's Force Preservation Council what circumstances warrant the suspension of access to classified material or processing for revocation of security clearance.

5. Contracting Officer's Security Representative (COSR). All commands which award contracts to industry requiring access to classified NSI by the contractor and employees, or which shall result in the development of classified NSI and/or equipment shall appoint, in writing, one or more qualified security specialists as COSR for security.

a. Details concerning this requirement are contained in Chapter 6 of this Order.

b. Contracts with SCI performance of work requirements must be coordinated with the Command SSO, approved by the Command's Senior Intelligence Officer and sent to SSO Navy and the Intelligence-Related Contract Coordination Office before SCI access is granted to contracted personnel.

6. Inspections, Assessments, and Reviews

a. Commanding Officers shall conduct inspections, assessments, and reviews to examine overall security posture of subordinate commands. Inspections or reviews of subordinate commands shall be conducted annually unless operational commitments prevent such action. IGMC inspections are no-notice.

b. Commanding Officers are responsible for evaluating the security posture of their subordinate commands. This includes developing an understanding of challenges subordinate commands have regarding execution of the requirements of this program and promulgating all information obtained from senior level commands.

7. SSA. Commands may perform specified security functions for other commands via SSA. Such agreements may be appropriate in situations where security, economy, location, and efficiency are considerations.

a. These agreements must consider the full spectrum of security services.

b. Considerations in developing the SSA include the capabilities and requirements of each participating command, and the command relationships that may or may not exist.

c. SSA shall be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement shall include requirements for advising Commanding Officers of any matters which may directly affect the security posture of the command.

d. SSA should also include comments regarding funding for any additional inspections or Temporary Additional Duty (TAD) that may be incurred because of the agreement.

e. Append any SSA to the affected command security instruction.

8. Planning for Emergencies

a. All commands, squadron/battalion level and above, shall establish an EAP for the protection and removal of classified NSI under its control during emergencies.

b. EAP should be sufficiently generic as to support the destruction of classified NSI in any potential situation. Only those materials resident within the confines of the command shall be used/planned for to support the Electronic Devices and Systems security system.

9. Annual Reporting Requirements. Reference (d) mandates reporting several items of information to support the Department of the Navy's requirement for oversight of the Marine Corps IPSP.

a. Command's will utilize AGENCY SECURITY CLASSIFICATION MANAGEMENT PROGRAM DATA STANDARD FORM 311 for annual submission. STANDARD FORM 311 can be downloaded at http://www.gsa.gov/portal /portal/forms/download/116190.

b. Data shall be consolidated at the MCINCR-MCBQ and reported to the MARFOR/Marine Corps Installations Command level for all subordinate commands and submitted to HQMC PS no later than 45 days past the end of the previous fiscal year. Report Control Symbol (RCS) 5510-22 (External RCS DD-INT(AR)1418) is assigned to this reporting requirement.

Chapter 3

Security Education

1. Basic Policy. Commanding Officers shall establish and maintain an active security education program to instruct all personnel in security policies and procedures, regardless of their position, rank, or grade.

a. The purpose of the security education program is to:

(1) Ensure that all persónnel understand the criticality of, and procedures for prótecting classified NSI.

(2) Increase security awareness for personnel throughout the command.

b. The goal is to develop fundamental security habits as a natural element of each task.

c. Security training must be sufficiently diverse and interesting to ensure that it is not viewed as too drudgery to complete.

d. All other requirements remain as outlined in reference (d).

Chapter 4

Information Security

1. Basic Policy. Commanding Officers shall ensure that all classified NSI entrusted to their command is protected per the provisions of this Order and references.

a. Personnel assigned to the command permanently or TAD, shall not be granted access to such material unless appropriately cleared according to references (b), (c), and Chapter 5 of this Order.

b. A Need-to-Know determination shall be made by the Commanding Officer prior to granting access to classified material.

c. At no time shall rank and position be the sole considerations for granting access.

d. Classified NSI shall be stored only in General Services Administration (GSA) approved security containers, in approved areas, on accredited IT systems and under conditions which prevent unauthorized persons from gaining access. This includes securing the material 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 NSI is processed or stored.

(1) Areas designated as Open Storage shall be designated, in writing, by the Command Security Manager or Commanding Officer, as restricted areas following the completion of a Physical Security Survey (PSS) conducted in accordance with reference (d).

(2) All personnel shall comply with the Need-to-Know policy for access to classified NSI.

e. Classified NSI is the property of the U.S. Government and not personal property.

(1) Military, government civilian employees and contractors who resign, retire, or otherwise separate from the Marine Corps, shall return all classified NSI in their possession or in security containers over which they exercise control to the command from which received, or to the nearest Marine Corps command prior to accepting final orders or separation documents.

(2) All courier cards and hand-carry authorizations shall be returned to the authorizing Command Security Manager or SSO, or to the Command Security Manager or SSO at the appropriate Command nearest the location of the Marine or civilian who is departing Naval Service.

2. Classification Management

a. All commands possessing or authorized to receive and maintain classified NSI shall develop a Classification Management Program that describes and supports creation, marking, control, dissemination, and destruction of classified material in accordance with reference (c).

b. Across the government, many classification actions are derivative in nature. Any person with appropriately assigned clearance eligibility and approved access may act as a derivative

classifier. To support this authority, reference (c) established several requirements to ensure a better process.

(1) Derivative classifier training shall be conducted and documented initially for anyone within a command who has access to classified NSI and annually thereafter for as long as the individual has access to classified NSI. If refresher training is not conducted within 12-months, derivative classifier authority shall be suspended for that individual until the training is conducted.

(2) The name of the person creating the derivative document must be placed on the derivatively created document. Reference (a) provides specific guidance.

(3) Identification of multiple sources used to derivatively classify a document shall be included on or with the document and retained during its lifetime.

3. Applicability of Control Measures. Classified NSI shall be afforded a level of control commensurate with its assigned security classification level. This policy encompasses all classified NSI regardless of storage location or media (e.g., removable or removed classified hard disk drives, external hard drives, computers, disks, documents, etc.).

4. Secret and Confidential Control Measures

a. Commanding Officers shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical (e.g., software, hardware, or firmware), physical (e.g., physical barriers, locks, security containers, Intrusion Detection System, etc.), and personnel control measures (e.g., investigations, access, need-to-know, visit certifications. etc.). Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers shall be submitted in accordance with Chapter 1, paragraph 6 of this Order.

b. Classified material, Secret and below, stored and maintained in an area designated as Open Storage requires no additional control provided the material does not leave the confines of the Open Storage area. Material taken from the Open Storage area must be controlled and accounted for until returned.

c. Classified material stored in a security container in an area designated as Closed Storage must be controlled and accounted for until returned.

d. Classified material stored in a GSA approved security container located outside of an area designated as a Level One, Two or Three Restricted Area, shall be inventoried a minimum of once per year (i.e., annual clean-out) and the inventory retained for the life of the document, plus two years.

5. Classified Hard Disk Drives (HDD). Classified HDD shall be inventoried and controlled with a locally developed control number and stored in a location suitable for the storage of the level of classification for the information contained on the HDD.

6. Working Papers. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents.

a. 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. Care should be taken to ensure source material relates to the Working Papers so that at the 180-day point, appropriate markings and source material association can be made.

b. Working papers shall be:

(1) Dated when created.

(2) Conspicuously marked as Working Papers on the first page in letters larger than the document text.

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

(4) Protected per the assigned classification level.

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

c. Email, blog, and Wiki entries, bulletin board posting, and other electronic messages properly transmitted on classified networks within or external to the originating activity shall be marked as required for finished documents, not as working papers.

7. CUI Control Measures

a. In accordance with MARADMIN 664/20, CUI (i.e., For Official Use Only) is unclassified information that requires dissemination control to preclude unauthorized public release and unauthorized disclosure of the information.

b. The holder of CUI has the final responsibility for determining whether an individual has a valid need for access to the information.

c. CUI documents may be destroyed by any of the means approved for the destruction of classified NSI or by any other means that would make it difficult to recognize or reconstruct the information.

d. For more guidance and regulations on CUI refer to reference (e).

8. Security Violations. The Commanding Officer shall ensure a Security Inquiry (SI) is conducted, in accordance with the requirements outlined in references (a), (c), and (d) of this

Order. When a loss or unauthorized disclosure of classified NSI, to include electronic spillages, is suspected, an SI is mandatory.

a. Failure to follow procedures that prevent a loss or unauthorized disclosure also require an SI.

b. The purpose of the SI is to, at a minimum, determine and report within 10 duty days:

(1) If a loss or unauthorized disclosure occurred.

(2) Extent of the loss or unauthorized disclosure.

(3) Potential damage to national security.

c. 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 an SI. The command official shall have:

(1) Eligibility and access commensurate with the classification level of the information involved.

(2) The ability to conduct an effective, unbiased investigation.

d. The Command Security Manager or SSO, in conjunction with the appropriate legal authority, shall support the SI process to:

(1) Ensure the investigation is conducted.

(2) Ensure the appropriate actions are taken to negate or minimize damage to national security; and to prevent future violations.

(3) Upon the initiation of the SI, notify the MCB Quantico NCIS field office who shall determine their level of involvement. Additional guidance can be obtained from reference (c).

9. Destruction of Classified Material. Commanding Officers shall establish procedures to ensure that all classified material intended for destruction is destroyed by authorized means and by appropriately cleared personnel.

a. An annual clean-out day shall be established where specific attention and effort are focused on disposition of unneeded classified material.

b. Destroy classified NSI no longer required for operational purposes per reference (a), Vol. 3, and this Order.

10. Foreign Disclosure. Although not strictly a security function, the Designated Disclosure Authority, Foreign Disclosure Officer, and Command Security Manager shall be informed of all incoming and outgoing foreign visits within the command. Command SSOs must be informed 24 hours in advance for all foreign visits within SCIFs. For additional guidance refer to reference (d).

Chapter 5

Personnel Security

1. Basic Policy. Requests for PSI shall only be submitted on individuals in cases where a bona fide requirement exists for access to classified NSI or occupation of a sensitive position/position of trust.

a. This must be substantiated by:

(1) Billet/MOS requirements.

(2) Current directive.

(3) PD.

(4) BIC.

(5) Permanent Change of Station/Permanent Change of Assignment orders.

(6) Individual Augmentee billet orders.

(7) Public law or other policy manual.

b. The PSI shall not be submitted based on the following:

(1) Individual desire.

(2) Convenience.

(3) Prior investigation.

(4) To support infrequent facility access where an escort is feasible.

2. Additional guidance is contained in reference (d).

Chapter 6

Industrial Security

1. Basic Policy. Commanding Officers shall establish an industrial security program within their command if the command engages in classified procurement or when cleared DoD contractors operate within areas under their direct control.

a. Reference (a) provides specific guidance for the release and sharing of classified NSI with authorized contractors. This Order implements the requirements of reference (a).

b. Command security procedures shall include appropriate guidance, consistent with references (a) through (d), and this Order, to ensure that classified NSI released to industry is safeguarded appropriately.

2. Additional guidance is contained in reference (d).

Chapter 7

NATO Program

1. Basic Policy. Refer to reference (d) for more detailed guidance.

a. All individuals being read into access for classified information (at all levels) must be briefed on NATO.

b. Only individuals detailed by their billet (Refer to OF-8, TO&E, and MOS Manual) can be read into NATO access (at any level).