UNITED STATES MARINE CORPS
MARINE CORPS UNIVERSITY
EDUCATION COMMAND
2076 SOUTH STREET
QUANTICO, VA 22134-5129

IN REPLY REFER TO:
5510
SEC
OCT 0 7 2019

EDUCATION COMMAND ORDER 5510.1

From: Commanding General
To: Distribution List

Subj: EDUCATION COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) DoDM 5200.01 Volumes 1-4, DoD Information Security Program of 24 Feb 12
(b) DoD Manual 5200.02 dtd 3 April 2017
(c) DoD Manual 5220.22 dtd 28 February 2006
(d) SECNAVINST 5510.30
(e) SECNAVINST 5510.36B
(f) MCO 5510.18B
(g) TECOM Order 5510.1
(h) PDUSD Memo, DoD Security Lexicon dtd 13 June 2013
(i) SECNAV M-5210.1
(j) MCO 5530.14A
(k) TECOM Order 5510.2A
(l) JAGINST 5800.7F
(m) ALNAV 001/16

Encl: (1) Information and Personnel Security Policy

1. Situation. Per the references, Education Command (EDCOM) is required to publish a command security instruction to provide guidance and instructions for the management of the Information and Personnel Security Program (IPSP).

2. Mission. To publish policies, responsibilities, and standards for the administration of the EDCOM IPSP as required by references (a) through (g).

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All EDCOM HQ personnel shall comply with the contents of this order in order to ensure the security and protection of information and the management of personnel security in accordance with all applicable references.

(2) Concept of Operations

(a) The EDCOM Security Manager will:

1. Administer the IPSP on behalf of the Command General (CG).

2. Conduct periodic reviews and inspections of the EDCOM IPSP.

(b) All colleges, schools, and sections will be familiar with the contents of this order and, where applicable, will follow the guidance and directions pertaining to IPSP as given by the EDCOM Security Manager.

b. Tasks

(1) Vice President for Business Affairs. Provide oversight and supervision of the IPSP.

(2) EDCOM Security Manager.

(a) Manage the EDCOM IPSP.

(b) Ensure all personnel responsible for the protection of classified national security information (CNSI) and/or controlled unclassified information (CUI) are familiar with the contents of this order.

(c) Ensure all personnel (permanent personnel and students) are screened upon arrival to ensure the Commander is fully aware of the member's personnel security investigation (PSI) status and any potential derogatory issues.

(d) Ensure all appointed Assistant Security Managers attend the USMC Security Management Course.

(e) Per reference (a), establish administrative procedures for the internal control of CNSI in order to protect CNSI from unauthorized disclosure.

(f) Develop an Emergency Action Plan (EAP) for the protection of CNSI and CUI. The plan must be detailed with specific procedures and responsibilities based on your command's risk posture. If required, an emergency destruction plan will be incorporated into the EAP.

c. Coordinating Instructions

(1) This Order is to be the primary source to ensure standardization of the IPSP. If conflicts arise between this Order and the various Department of Defense (DoD) and Department of the Navy (DON) information and personnel security references, the DoD information and personnel security references provide the final guidance.

(2) All personnel will be made aware of the location and how to contact the Security Manager.

(3) Coordinate all information or personnel security issues, concerns, or matters with the EDCOM Security Manager.

4. Administration and Logistics

a. Recommendations concerning the content of this Order should be forwarded to the EDCOM Security Manager.

c. Records created as a result of this Order shall be managed according to reference (i), to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium.

5. Command and Signal

a. Command. This Order is applicable to all EDCOM total force.

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

JM Bargeron
J. M. BARGERON

DISTRIBUTION: A

LOCATOR SHEET

Subj: EDUCATION COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Location: ____

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

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of person Incorporating Change

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

CHAPTER 1

INTRODUCTION

1000. Basic Policy. The EDCOM IPSP is established to ensure CNSI and CUI are protected from unauthorized disclosure.and the granting of access to CNSI is clearly consistent with the interest of National Security. This Order supplements applicable portions of the references which support the implementation of the EDCOM IPSP.

1001. Authority. The CG, EDCOM is responsible for establishing and maintaining an IPSP in compliance with references (a) through (f). The EDCOM Security Manager, hereafter referred to as "Security Manager," is responsible for ensuring there is an effective program and it complies with all directives issued by higher authority.

1002. Responsibility

1. EDCOM Vice Presidents, Directors, and Section Heads are directly responsible for ensuring compliance with this Order. They will ensure all personnel are informed of their responsibilities to safeguard CNSI and CUI or equipment entrusted to them. They will ensure only the minimum number of personnel who possess the appropriate security clearance "eligibility," a valid "need-to-know," and the "required training," are authorized access to CNSI.

2. Each individual, military, civilian, or contractor, is responsible for the handling and protection of CNSI and CUI to which access has been granted. Each individual is responsible for reporting any violation of security regulations or security weaknesses to the CG and Security Manager.

3. EDCOM supervisors, at all levels, are responsible for ensuring the performance rating system of all EDCOM military and civilian personnel, whose duties significantly involve the creation, handling, or management of CNSI, include a critical security element on which to be evaluated.

1003. Applicability. This Order establishes policies for the protection of CNSI and CUI, and personnel security matters incorporating numerous DoD and DON policies. It is not expected that these directives will or can ensure absolute security of EDCOM. Rather, they permit the accomplishment of essential tasks while affording selected items of information a reasonable degree of security with minimum risk.

1004. Assistance via the Chain of Command. EDCOM personnel are required to obtain collateral and SCI related guidance or policy interpretation from the Security Manager's office.

1. Telephone inquiries may be made at (703) 432-5578, (703) 432-4787, or (703) 784-0094. (TECOM SECURITY MANAGER)

3. Under normal circumstances, EDCOM personnel will not directly contact HQMC Plans, Policy and Operations (PP&O) or the Deputy Under Secretary of the Navy (Security & Intelligence), for any reason.

4. Under normal circumstances EDCOM personnel will not contact MCIA directly.

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. Management Officials

1. Commanding General. An effective IPSP relies on a team of professionals working together to fulfill the CG's responsibilities. The CG's responsibilities are outlined in reference (f).

2. Security Manager. The Security Manager will be appointed, in writing, by the CG, in accordance with reference (f). The duties of a Security Manager are delineated in references (a), (d), (e), and (f).

3. Assistant Security Manager(s). The Assistant Security Manager will be appointed in writing. The Assistant Security Manager assists the Security Manager in fulfilling the CG's responsibilities for the protection of CNSI and CUI in accordance with references (a) through (f). The Assistant Security Manager reports directly to the Security Manager for guidance, direction, coordination, training and oversight necessary to ensure the program is being administered effectively.

4. Other Security Appointments

a. Contracting Officer's Security Representative (COSR). If required, the commander will appoint a COSR, in writing, per reference (f). Currently, the TECOM Security Manager is responsible for Industrial Security.

b. Top Secret Control Officer. Per references (a) and (f), a TSCO is required when the command holds Top Secret material. The Security Manager will hold this appointment.

c. North Atlantic Treaty Organization (NATO) Control Officer. Marine Corps Combat Development Command (MCCDC) maintains the NATO account for MCB Quantico, which includes appointments as a Control Officer.

e. Foreign Disclosure Officer. In accordance with reference (k), the CG will appoint a primary Foreign Disclosure Officer (FDO), to manage the Foreign Disclosure Program within EDCOM. The FDO responsibilities pertaining to this order are to; ensure Marine Corps foreign disclosure and release actions; and provide foreign disclosure oversight for all foreign nationals assigned to EDCOM in accordance with applicable directives, regulations, instructions, and orders and maintain all foreign disclosures records.

2001. Security Servicing Agreements. In accordance with reference (f), commands are authorized to perform security functions for another command and vice versa, via a Security Servicing Agreement (SSA). Refer to reference (f) when developing a SSA.

2002. Inspection, Assessment, and Review Program.

1. The CG is responsible for evaluating the security posture of their subordinate commands. Inspections, assessments, and reviews will be conducted by the Security Manager's office and will inquire into the security procedures and practices including, but not limited to, classification management, transmission and transportation, access, storage, security education and training, using the HQMC Functional Area Checklist (5510.3).

2. Per references (a), (d), and (e), EDCOM will conduct annual self-inspections of the IPSP. Any discrepancies will be addressed immediately and reported via the chain of command not later than 14 days following the inspection.

2003. Inventory of Classified Material

1. General. An inventory of all classified material will be conducted annually by the Security Manager, Assistant Security Manager, or appointed Secondary Control Point (SCP) Custodian. Such inventories will involve a reconciliation to ensure that all material received by the Command is, in fact, physically on hand and administrative records are current and accurate.

a. Annual inventory reports are due the 30th day of April each year.

b. Annual inventory reports will consist of an updated inventory spreadsheet or roster, with a cover letter signed by the Security Manager or authorized signature authority.

2. Frequency of Inventory. In addition to annual inventories, an inventory will be conducted on the following occasions:

a. When there is a change of Security Manager.

b. When a security container is found open, unattended, and compromise or suspected compromise has occurred.

c. When a member of the command having access to the classified material commits suicide, attempts suicide, or is in an unauthorized absence status for 48 hours.

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

3000. Basic Policy. Certain matters affecting national security must be reported to the Naval Criminal Investigation Service (NCIS). All personnel, whether they have access to CNSI or not, will report to the commander, Security Manager, or nearest command, any activities described in this chapter involving themselves, dependents, co-workers, or others. The commander and/or the Security Manager will notify NCIS immediately.

3001. Sabotage, Espionage, Terrorism, Subversion, or Deliberate Compromise

1. All personnel must comply with the requirements in reference (d).

2. NCIS will advise what additional action(s) are to be taken and will effect liaison and coordination with appropriate members of the U.S. intelligence community.

3002. Contact Reporting

1. All personnel who possess a security clearance are to report to the Security Manager, contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's activities in which illegal or unauthorized access is sought to CNSI or otherwise sensitive information.

2. All personnel must report to the Security Manager if they are concerned they may be the target of exploitation. On behalf of the CG, the Security Manager will review and evaluate the information and promptly report it to NCIS.

3003. Suicide or Attempted Suicide, Unauthorized Absentees, Death, or Desertion. All personnel must comply with the requirements in reference (d).

3004. Foreign Travel and Foreign Connections. All personnel must comply with the requirements in reference (d).

CHAPTER 4

SECURITY EDUCATION, TRAINING, AND AWARENESS

4000. Basic Policy and Responsibility. The Security Manager is responsible for establishing and maintaining a robust security education program to instruct personnel in security policies and procedures, regardless of their position, rank, or grade.

4001. Purpose. The purpose of the IPSP security education, training, and awareness (SETA) program is to ensure all personnel understand the need to handle and protect CNSI and CUI. The goal is to develop fundamental habits of security so proper discretion and judgment will automatically be exercised in the discharge of duties involving CNSI.

4002. Scope. SETA will be provided to all EDCOM personnel granted access to CNSI.

4003. Minimum Requirement. The following are the minimum SETA requirements.

1. Indoctrination Brief. All personnel who are granted access to CNSI must maintain a basic understanding of what CNSI is, and why and how CNSI is safeguarded. This training will be administered (hardcopy or electronically) to all personnel granted access to CNSI. Additionally, those individuals granted access to CNSI will also be required to complete and sign a SF-312, "Non-disclosure Agreement." The indoctrination brief includes those topics covered in references (a) through (f). The Security Manager will maintain copies of all SF-312s and indoctrination training certificates to confirm the training has taken place.

2. Orientation Brief. Each personnel who check into EDCOM will receive an orientation brief from the Security Manager or Assistant Security Manager. The brief will be tailored to address the specific security procedures and requirements within EDCOM.

3. On-the-job Training. Supervisors will ensure that subordinates know the security requirements that impact their duties. On-the-job training by supervisors and leaders will cover such aspects as proper use of SF 701, derivative classifier training, local access procedures for the work area, and protection of classified materials when not secured.

4. Annual Refresher Training. The Security Manager will develop an annual refresher brief for all personnel who have access to CNSI. The refresher training will be designed to reinforce security awareness and motivate security discipline on specific topics/issues as they arise. Changes in security policies and procedures, positive and negative trends noted in the command security program, and special security considerations, such as the processing of CNSI on computers, are examples of items to be covered during refresher training.

5. Counterintelligence Brief. All personnel will receive an annual counterintelligence brief by NCIS. The schedule will be promulgated by the EDCOM Security Manager.

6. Derivative Classification Training. All personnel who have access to CNSI and system, will complete derivative classification training annually. This training is located on the Center for the Development of Security Excellence (CDSE), Security Training, Education, and Professionalization Portal (STEPP) site at https://cdse.usalearning.gov/login/ index.php. Users will be required to create and maintain a STEPP account.

7. USMC Security Management Course. All appointed Security Managers and security specialist in EDCOM HQs must attend the USMC Security Management Course within 180 days of appointment.

a. The USMC Security Management Course is offered by a Mobile Training Team from HQMC, PP&O (PS) and Certified USMC Security Instructors. It provides Marine Corps specific information and discusses the day-to-day mechanics of managing a command's IPSP. Course registration is online only and is located at: https://eis.usmc.mil/sites/hqmcppo/PS/PSS/Blog /SitePages/SMC.aspx.

b. Prerequisites. Prior to registering for the USMC Security Management Course, security managers must complete the required prerequisites listed on the HQMC PP&O (PS) PSS Blog site. Additionally, these prerequisites are required to be completed 30 days after appointed regardless of scheduled USMC Security Management Course date.

CHAPTER 5

INFORMATION SECURITY

5000. Basic Policy. The CG shall ensure all CNSI entrusted to the command is protected per the provisions of this Order and references (a) and (f).

1. Personnel will not be granted access to CNSI unless appropriately cleared according to reference (f).

2. The Security Manager will validate "**Need-to-Know**" prior to granting access to CNSI, when required.

3. At no time will rank or position be the sole considerations for granting access.

4. CNSI will be stored only in a General Service Administration (GSA) approved security container, 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 CNSI is processed or stored.

a. Secure Rooms (SR) will be designated, in writing, by the TECOM Security Manager, following the completion of a Physical Security Survey (PSS) conducted in accordance with reference (j). All designated SRs must also be designated as a Restricted Area in accordance with reference (j).

b. All personnel will comply with "**Need-to-Know**" policy for access to CNSI.

c. Weapons or pilferable items such as money, jewels, precious metal, or narcotics will not be stored in the same security container used for the storage of classified material.

d. Classified material will also not be stored with UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY, or any other material.

5. CNSI is the property of the United States Government and not personal property.

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

b. The DD-Form 2501, "Courier Card" will be returned to the Security Manager's office prior to departing the command.

5001. Classification Management. EDCOM does not have Original Classification Authority. All classification actions within EDCOM are derivative in nature. In accordance with reference (f), any person with appropriately assigned clearance eligibility and approved access to CNSI may act as a derivative classifier. In order to support this authority, the following requirements must be met.

1. Training. Refer to chapter 4 of this Order for training requirements.

2. Marking. Mark all CNSI material derived within EDCOM in accordance with Volume 2 of reference (a) and paragraph 5004 of this Order.

5002. Custody and Accountability. The Security Manager will receive, route, and account for all CNSI addressed to, received, or retained at EDCOM.

1. All directorates, special staff, and sections that receive and retain CNSI are required to register as a SCP with the TECOM CMCC in coordination with the EDCOM Security Manager.

2. All classified material will be accounted for and barcoded by the TECOM CMCC and entered into the appropriate SCP inventory via the TECOM CMCC database.

3. The TECOM CMCC is not a holding facility for CNSI. Anytime material requires destruction or barcoding, the SCP Custodian is required to set up an appointment with the TECOM CMCC. If all necessary documents, material, etc., are not ready by the appointment, the SCP Custodian will be required to go back with the material and return at a later date.

5003. Applicability of Control Measures. CNSI will be afforded a level of control commensurate with its assigned classification level. CNSI will be controlled in accordance with reference (f) and the following:

1. TOP SECRET Controls. EDCOM will rarely handle or store CNSI at the TOP SECRET classification level. If required, all handling and/or storage of TS material will be coordinated with the EDCOM Security Manager.

2. SECRET and CONFIDENTIAL Controls

a. The Security Manager's office is a decentralized facility, which means, all classified material (including working papers) will be controlled, managed, and retained at the designated SCP. All classified material, hardcopy and mass media storage devices, at EDCOM or received from another command will be entered into the TECOM CMCC database.

b. All controlled documents leaving the Security Office to the SCP, will have with them two classified material control forms, which identifies the document(s). One copy of the control form is to be signed and dated by the SCP and retained as a receipt by the Security Manager until the document appears on the next reported inventory. The second control form is for use by the SCP for their local accountability requirements. Document control forms are UNCLASSIFIED and may be reproduced locally for that purpose.

5004. Working Papers

1. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items which are not finished documents. Working documents shall be created and managed in accordance with Volume 2 of reference (a).

2. Email, blog, and Wiki entries, bulletin board posting, and other electronic messages properly transmitted on classified networks within or external to the command will be marked as required for finished documents, not as working papers. Note: Information dynamic in nature (e.g., wikis and blogs) and not properly marked in accordance with Volume 2 of reference (a) are prohibited from use as source of derivative classification.

5005. Marking

1. All CNSI will be clearly marked with date and office of origin, the appropriate classification level and all required markings in accordance with Volume 2 of reference (a). The purpose of marking CNSI is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading, and declassifying actions.

2. Marking of Secret Internet Protocol Router Network (SIPRNet) e-mails and attachments will be in accordance with Volume 2 of reference (a). All documents identified as SIPRNet e-mail not conforming to the appropriate marking requirements will be considered a violation of security practices and will not be looked on favorably during inspections.

5006. Reproduction. CNSI will be reproduced only to the extent required by operational necessity unless restricted by the CG, or for compliance with applicable statutes or directives. Only an authorized person having knowledge of reproduction procedures will carry out the reproduction of CNSI.

5007. Transmission or Transportation. CNSI will be transmitted either in the custody of an appropriately cleared individual or by an approved system or courier, and in accordance with the Volume 3 of reference (a). The Security Manager will provide courier authorization letters and cards, as required.

1. Authorization to Escort or Handcarry CNSI. In accordance with Volume 3 of reference (a), the Security Manager will provide written authorization to all personnel escorting or handcarrying CNSI. This authorization can be the DD Form 2501, Courier Authorization Card, included on official travel orders, or a courier authorization letter. These authorizations will be

used to identify appropriately cleared DoD military and civilian personnel approved to escort or handcarry CNSI on the following conditions:

a. Individual has a recurrent need to escort or hand carry CNSI.

b. The expiration date may not exceed three years from the issue date (pertains only to the DD 2501).

c. The written authorization is retrieved upon an individual's transfer, termination of employment, or when authorization is no longer needed.

2. All escort and handcarry request will be submitted to the Security Manager's office for processing. Note: Courier authorization is not a guarantee and must be justified.

3. Approval to remove CNSI from the physical confines of the command must be approved by the Security Manager; however, should travel require an overnight stopover where no government facility to store the material is available, the hand carrying of CNSI will not be authorized.

4. All material being transported from the physical confines of EDCOM will be double-wrapped. A locked briefcase may serve as the outer cover, except when handcarrying aboard commercial aircraft.

5. Preparing CNSI for Shipment. All shipments of CNSI within EDCOM will be coordinated through the EDCOM Security Manager.

5008. Destruction of CNSI. All CNSI, within EDCOM, will be destroyed in accordance with Volume 3 of reference (a). For destruction of hardcopy CNSI material, only crosscut shredders listed on the National Security Agency/Central Security Service (NSA/CSS) Evaluated Products List for High Security Crosscut Paper Shredders may be used.

1. CNSI registered with the TECOM CMCC not in use should be turned over to the TECOM Security Manager's office for destruction.

2. Clean-Out Day. The CG, via the EDCOM Security Manager, is required to establish at least one day each year as a "clean-out" day. During this day, specific attention and effort is focused on disposition of unneeded CNSI and CUI. The annual clean-out day for EDCOM will be during January of each year.

3. All CNSI registered with the TECOM CMCC marked for destruction, must be returned to the TECOM CMCC for proper destruction and removal from the respective SCP's inventory.

5009. Dissemination of CNSI. Dissemination of CNSI outside the command must be approved by the CG, via the EDCOM Security Manager. CNSI originated in a non-DOD department or agency cannot be disseminated outside the DOD without the consent of the originator, except where specifically permitted.

5010. Dissemination of CNSI to Foreign Nationals. U.S. classified information is disclosed to foreign nationals only in accordance with reference (k). At no time will any member of EDCOM, regardless of status, provide U.S. CNSI to any foreign national without prior written approval from the EDCOM FDO.

5011. Physical Security Measures

1. Storage Requirements. CNSI will only be stored in those areas which have been evaluated and approved, in writing, by the Security Manager. CNSI will be stored in:

a. A GSA approved security container.

b. A Class A or B vault.

c. An approved secure room.

2. Security Containers. GSA establishes and publishes minimum standard, specifications, and supply schedules for security containers, vault doors, and modular vaults. Modification of any equipment used to store CNSI is prohibited. Contact the Security Manager for guidance on procurement of a GSA approved security container or vault door.

3. Secure Rooms. A secure room is a cleared building, room, or space for open storage of CNSI at the level designated by the Security Manager. All secure rooms must meet the requirements in the Appendix to Enclosure (3) of Volume 3 of reference (a), be designated, in writing, by the Security Manager, and have a PSS conducted every 18 months per reference (h). If CNSI technologies (i.e., SIPRNet) are included within the secure room, coordinate communications security with EDCOM Information Technology branch.

a. Only authorized cleared personnel will have access to secure rooms.

b. All personnel who are not on the access roster to the designated secure room are considered visitors and will utilize the visitor log, to include maintenance personnel. All visitors will be escorted at all times while in the secure room by an authorized person.

c. Each secure room will have a designated point of contact who works directly with the Security Manager in the management of the space and CNSI held within.

d. In the event of an emergency, law enforcement and emergency personnel are authorized access to all designated TECOM secure rooms. After access is no longer required, immediately notify the Security Manager. The Security Manager will handle all follow-on procedures. These procedures may include, but not limited to, inadvertent disclosure briefs and execution of a SF-312 and debrief forms.

4. <u>Combination Locks</u>

a. Combinations to security containers will be changed only by trained individuals having the responsibility and appropriate security clearance. The Security Manager will provide required training to designated personnel.

b. The combination will be given only to authorized personnel, who's official duties require access to the container or space.

c. Combinations will be changed when containers/locks are first placed in use, at least annually thereafter, and when any of the following occurs:

(1) An individual knowing the combination no longer requires access.

(2) The combination has been subject to possible compromise or the security container has been discovered unlocked or unattended.

(3) The container is taken out of service.

d. The Standard Form 700 (SF 700) will be used to record combination changes. The SF-700 is a form that contains vital information about the security container in which it is located. This information includes location, container number, lock serial number, and contact information if the container is found open and unattended. The SF 700 will list the personnel who have access to the combination and the detachable portion of the combination envelope will be attached inside the locking drawer. The Security Manager will maintain Part II of all executed SF 700s throughout the command. Personnel having access to the combinations must have eligibility and access granted equal to the classification of the combinations.

5. <u>Repairs To Damaged Security Containers</u>. A bonded locksmith is authorized to repair and replace parts on all security equipment and should be called upon when required. The Security Manager and EDCOM G-4 will be responsible for contracting a GSA approved bonded locksmith to make necessary repairs and will pay for such repairs using a Government Purchase Card (GPC). Under no circumstances will repairs be made or attempted by untrained personnel. All repairs or modifications must be recorded on an Optional Form 89. A properly cleared individual will be present at all times when maintenance is performed on security containers storing classified material.

5012. End of Day Checks. All Restricted Access Areas (RAAs), Controlled Access Areas (CAAs), and Secure Rooms (SRs) must use the SF-701, "**Activity Security Checklist**" to record security checks at the close of each duty and/or business day to ensure the area where CNSI is used or stored is secure. An integral part of the security check will be the securing of all vaults, secure rooms and containers used in storing CNSI. The SF-702, "**Security Container Check Sheet,**" will be used to record such actions. Both forms will be retained and disposed of as required by record management schedules.

5013. Security Incidents Involving CNSI. Protection of CNSI is essential to maintaining security and achieving mission success within the command. A security incident is identified as either a violation or infraction, based on the completion of a preliminary inquiry (PI) or investigation. All security incidents will require a PI, a command investigation, or both.

1. Infraction. An infraction is a security incident involving failure to comply with requirements outlined in this Order and all references associated, which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of CNSI.

2. Violation. A violation is a security incident which indicates knowing, willful, and negligent for security regulations, and results in, or could be expected to result in, the loss or compromise of CNSI. A PI will be conducted on all security violations.

a. Compromise. A security incident in which there is an unauthorized disclosure of CNSI.

b. Loss. When CNSI cannot be physically located or accounted for.

3. Electronic Spillage (ES). An ES occurs when CNSI or CUI is transferred onto an information system not authorized for the appropriate security level or not having the required protection or access controls. A spillage creates the potential for further widespread unauthorized disclosure of that information, including to the Internet. Examples of an ES of classified information: Secret information processed on and/or transmitted via NIPRNET, TS/SCI information processed on and/or transmitted via SIPRNET. Examples of an ES of CUI: For Official Use Only information posted to a publicly accessible website or forwarded to a personal email address.

a. All ESs will be reported to the EDCOM Security Manager, EDCOM Information Technology, and TECOM G-6 Cyber Security Branch, immediately, for reporting and clean-up purposes.

b. ESs will be processed in accordance with reference (m).

4. Preliminary Inquiry (PI). A fact-finding analysis conducted to determine whether or not there was a loss of CNSI or whether or not unauthorized personnel had, or could have had, access to

the information. When CNSI has been lost, compromised or subject to compromise, the following will happen.

a. CG will appoint, in writing, a PI officer to conduct the SI.

b. Every effort will be made to keep the PI UNCLASSIFIED.

c. Specific guidelines for conducting a PI are contained in reference (f). The SI officer will consult the Staff Judge Advocate (SJA) and Security Manager before initiating the inquiry.

d. The PI will be completed within 10 working days.

e. NCIS will be notified of all security violations and their actions will be outlined within the PI.

f. Corrective actions will be taken by the Security Manager to prevent recurrence, if the PI does not reveal a loss or compromise of CNSI, but does reveal a weakness in security practices or established security procedures.

g. If the PI reveals a loss or compromise of CNSI is likely to have occurred, and/or disciplinary action is being considered or recommended, the CG must conduct a command investigation.

5. Command Investigation. The command investigation is an administrative proceeding conducted in accordance with section 0209 of reference (l). The purpose of the command investigation is to answer, in detail, "who, what, where, when, why, and how" questions concerning the security violation. The investigating officer will consult with the SJA before initiating a command investigation.

6. Compromise through Public Media. Individuals becoming aware that CNSI may have been compromised as a result of disclosure in the public media will immediately notify the EDCOM Security Manager. Those individuals should include as many details as possible, such as the name of the reporter, newspaper, television show, Internet address, dates, etc., to the EDCOM Security Manager. In turn, the EDCOM Security Manager will brief the appropriate personnel, on the specifics of the potential compromise and report the compromise to CG, TECOM (Security Manager) in accordance with reference (e).

7. Security Incidents or Unauthorized Disclosure Involving Foreign Governments. In accordance with reference (k), compromises of U.S. CNSI to foreign governments shall be promptly reported to the originating Marine Corps component and HQMC PP&O (PLU) via the TECOM FDO. The originating Marine Corps component will conduct a PI and damage assessment and forward results to HQMC PP&O (PLU) and (PS), for reporting to the National Disclosure Policy Committee via Navy International Policy Office.

8. Unsecured Security Containers. A major security violation occurs when a security container, which CNSI is stored in, is found unsecured in the absence of assigned and cleared personnel. If such an incident occurs, the EDCOM Security Manager will be notified immediately.

9. Unsecured Classified Material. When an item of CNSI is found unsecured, the finder will immediately notify the TECOM Security Manager for further instructions.

5014. Emergency Action Plans. Per reference (f), the CG is required to develop an EAP for the protection of CNSI and CUI in case of a natural disaster or civil disturbance. The EAP can be prepared in conjunction with the command's disaster preparedness plan.

CHAPTER 6

PERSONNEL SECURITY

6000. Basic Policy. The EDCOM Security Manager is responsible for management and implementation of the Personnel Security Program on behalf of the CG and in accordance with references (b), (d), and (f).

6001. Personnel Security Investigation (PSI)

1. No personnel will be given access to CNSI or be assigned to sensitive duties unless a favorable personnel security eligibility determination has been made regarding his/her loyalty, reliability, and trustworthiness. A PSI is conducted to gather information pertinent to these determinations.

a. Only the EDCOM Security Manager and/or those personnel specifically authorized to do so will request a PSI.

b. A PSI will not be requested on any individual who will retire, resign, or separate with less than one year of service remaining.

2. All military personnel are required to have a completed Tier 3 (T3) security investigation, regardless of military occupational school (MOS) or billet, per reference (b).

3. At a minimum, all civilians are required to have a Tier 1 (T1) suitability investigation completed prior to hiring by their human resources office (HRO). Security investigations processed on civilian employees are determined by the position sensitivity level (i.e., Special Sensitive, Non-Critical Sensitive).

a. Civilian sensitivity will not be downgraded solely to facilitate recruitment or retention of personnel or to accommodate adverse security determinations.

b. There are three levels of sensitivity, which pertain to civilian personnel in national security positions: Special Sensitive, Critical Sensitive, and Non-critical Sensitive, as described in reference (b).

4. All personnel who require a Common Access Card (CAC) must have, at a minimum, a T1 suitability investigation submitted with favorable fingerprint cards.

5. Per reference (f) all Formal School Instructors (military, civilian or contractor) must have, at a minimum, a favorably adjudicated T3 or T3 reinvestigation (T3R) security investigations prior to instructing students.

6002. Requests for PSIs. The EDCOM Security Manager tracks all EDCOM billets which require PSIs. A security representative will make contact with the individual directly when an initial PSI or reinvestigation is needed.

6003. Verification of Security Investigations. Verification of personnel security investigations will be conducted using the security system Joint Personnel Adjudication System (JPAS) or its successor system. The Security Office can provide a "verification of security investigation" letter to individuals within the command for military retention or federal employment.

6004. Access

1. Access Authority. The Security Manager, on behalf of the CG, grants access to CNSI up to and including TOP SECRET.

2. The Security Manager, on behalf of the CG, can deny or withdraw access to CNSI for cause via JPAS or successor system.

3. Adjudication of derogatory information concerning civilian and military personnel falls within the sole responsibility of the Department of Defense, Consolidated Adjudication Facility (DoDCAF) Navy.

4. Should an allegation be so severe as to question the individual's immediate or continued access to CNSI (e.g., felony charges), the Security Manager may immediately terminate the individual's access. This decision will be endorsed by the CG as soon as possible.

5. Temporary Access may be granted locally pending adjudication by DoDCAF Navy. The Security Manager, on behalf of the CG, is authorized to grant temporary access up to and including TOP SECRET, when the following conditions apply:

a. No derogatory information is present in the individual's security file or Questionnaire for National Security Positions (SF 86).

b. A PSI, at the appropriate level, has been opened by OPM via JPAS, or successor system.

c. A local records check is completed.

6. Request for Access. Prior to granting access to CNSI, a **"Request for Access"** package must be submitted to the Security Office for review and processing. All requests are based on the members Billet Identification Code (BIC) data. Requests for access at a higher level than the BIC position sensitivity level will require detailed justification to support the "**need to know**" requirement for the level of access requested and an approved Table of Organization and Equipment (TO&E) Change Request (TOECR). All **"Request for Access"** packages must include the following:

a. Access to TOP SECRET:

(1) Favorably adjudicated T5, T5R, or its equivalent.

(2) A local records check (LRC) is required when the Tier 5 (T5) or T5 reinvestigation (T5R) close date is older than 30 months, or when temporary access is warranted. Details of any adverse information discovered during the LRC will be forwarded by separate correspondence to the CG, TECOM (ATTN: Command Security Manager).

(3) An "Access Screening Checklist" will be completed when the PSI is less than 30 months old. The checklist will be retained in the member's personnel security file until the conclusion of his/her next T5R.

(4) An SF-312, "CNSI Non-disclosure Agreement," if not already executed and recorded in JPAS or successor system.

(5) An attestation declaration not previously recorded in JPAS.

(6) Signed NATO certificate brief.

(7) Completed training requirements (i.e., indoctrination and derivative classification).

b. Access to SECRET or below:

(1) Favorably adjudicated T3, T3R, or its equivalent.

(2) An SF-312, "Classified Information Non-disclosure Agreement," if not already executed and recorded in JPAS or successor system.

(3) Signed NATO certificate brief.

(4) Completed training requirements (i.e., indoctrination and derivative classification).

6005. Debrief

1. When an employee is removed, terminated, resigns, retires, or is reassigned to a position not requiring access, the Security Manager will ensure that a Security Termination Statement, OPNAV 5511/14 is executed and debriefings are conducted.

2. Individuals who transfer, PCS, or PCA will be debriefed accordingly.

6006. Joint Personnel Adjudication System

1. The Security Manager and Assistant Security Manager will have account manager and level 5 JPAS accounts.

2. The Security Office will maintain a JPAS Security Management Office (SMO) code.

3. All civilian, military, and contractor personnel must be owned or serviced via JPAS by the command.

4. JPAS notifications will be checked on a regular basis for messages from DoDCAF Navy.

5. Cleared DoD contractors and personnel TAD/TDY to EDCOM will be "serviced" in JPAS for the length of their contract or TAD/TDY. Servicing will not be longer than one year at a time.

6. JPAS Account Requests. The Security Office will only grant JPAS accounts to appointed security specialists within TECOM and its MSCs. Prior to granting an account, the following items must be completed and submitted to the TECOM Security Manager for processing:

a. DD Form 2962, Personnel Security System Access Request (PSSAR),

b. CDSE STEPP, JCAVS User level 2-6 course completion,

c. DoD Personally Identifiable Information course completion, and

d. DoD Cyber Awareness Training course completion.

7. All account holder JPAS PSSAR forms will be kept, electronically, as long as the accounts are active.

8. JPAS PSSAR forms will be kept for two years after accounts are deleted.

6007. Electronic Questionnaires for Investigations Processing (e-QIP) system

1. The EDCOM Security Manager will have e-QIP Direct account.

a. Prior to issuance of an e-QIP Direct account, users must request for a National Background Investigation Bureau (NBIB) Public Portal (NP2) account. NP2 account requests are processed by the Security Manager and require the below:

(1) Personal Identity Verification (PIV) authentication established.

(2) NP2 spreadsheet (located on the TECOM Security VCE Sharepoint Security site).

b. Due to system login requirements, it is imperative that e-QIP be logged into every two weeks. Accounts within e-QIP must be renewed every year. Not following these steps will lead to accounts being locked or terminated.

c. Personnel who no longer require access to e-QIP Direct, must have their e-QIP account immediately removed.

d. Maintenance of you assigned e-QIP Direct account is paramount in ensuring PSIs are properly initiated, reviewed, and submitted, and personnel who no longer require an account, no longer have it.

6008. Defense Information System for Security (DISS). DISS, once fully deployed, will replace JPAS, to serve as the system of record to perform comprehensive personnel security, suitability and credential eligibility management for all military, civilian and DoD contractor personnel. DISS provides secure communications between Adjudicators, Security Officers, and Component Adjudicators in support of eligibility and access management.

1. All Security Managers must obtain and maintain a DISS account for their command. Accounts are issued by the Security Manager. Accounts will only be issued to appointed security personnel (i.e., security manager, security assistants)

2. Each account request will include a DISS Security Officer Admin appointment letter, PSSAR, and training certificates.

6009. System Authorization Access Requests (SAARS). The Security Manager is only responsible for filling out the "Security Manager Validates the Background Investigation or Clearance Information" part of a SAAR form.

1. If a SAAR is for a classified system (i.e., SIPRnet) the Security Manager must validate the individual's derivative classification training, access to CNSI is granted via JPAS, and a NATO brief has been completed prior to filling out the "Security Manager Validates the Background Investigation or Clearance Information" part of a SAAR form.

2. Information Technology (IT) level designations are based on the individual's BIC and is the responsibility of the individual's supervisor or G-6, not the Security Office. If the individual is not in a billet with an IT level of I or II, the Security Office will not process a SAAR form for a classified system or database.

6010. Visitor Control. Visitors to the command for classified visits are required to have their Security Official submit a Visit Access Request (VAR) via JPAS to the Security Manager for approval. The Security Office will take necessary steps to verify the visitor's clearance and access level via JPAS. If the visitor's clearance and access level cannot be verified the classified visit will be disapproved. Departments/divisions and sections sponsoring the visit are responsible for maintaining coordination with the Security Office for the duration of the visit. A visitor's request is not required for unclassified visits.

1. Identification

a. Any visitor who is authorized access to classified material must present adequate identification at the time of the visit. Users of classified material will not permit access to classified material until they are satisfied as to the identity, security clearance, and the "need to know" status of the visitor as established by the Security Manager. In no case will users issue CNSI to visitors without written or verbal authorization from the Security Manager.

b. Access to classified material will not be permitted to foreign visitors unless approved by the EDCOM FDO prior to visit.

c. Access to classified material will not be permitted to DoD cleared contractors unless specifically authorized by the EDCOM Security Manager.

d. If doubt exists about granting access to any visitor, contact the EDCOM Security Manager.

2. Visitor Access Requests outside EDCOM. When personnel are required to make a classified visit to an outside unit, the individual traveling will inform the Security Manager at least one week prior to the visit. The Security Manager will verify the information and forward a completed visit request to the command to be visited via JPAS. The individual traveling will inform the Security Manager of the following information:

a. The individual traveling will inform the Security Manager of the following information:

(1) SMO code of command to be visited.

(2) Dates of visit.

(3) SSN or DOD EDIPI and Date of Birth of all personnel traveling.

(4) A point of contact for visit; name and phone number. This should not be the Security Manager at the command.

(5) Purpose of the visit.

(6) Classification level of visit.

b. When sending the above information, the following must happen:

(1) Email must be digitally signed and encrypted using DoD approved PKI certificates.

(2) Include “FOUO” in the subject line.

(3) Properly mark the body of the email in accordance with Volume 4 of reference (a).

(4) Do not “reply all” or “forward” emails containing FOUO or Personal Identifiable Information, unless ALL recipients have a valid “need-to-know” for the information within the email.

CHAPTER 7

CONTINUOUS EVALUATION PROGRAM

7000. Policy. As directed in reference (f), the Security Manager, on behalf of the CG, will report questionable or unfavorable information that may be relevant to the 13 adjudicative guidelines to DoDCAF Navy regarding members of the command based on recommendations made by the Security Manager.

1. Individuals must report to their supervisor or Security Manager any situation that fits within the guidelines covered in reference (d). Co-workers have an obligation to advise their supervisor or Security Manager when they become aware of adverse information concerning an individual who has an assignment to a sensitive position. The supervisors are mandated to forward such information to the Security Manager. The Security Manager will report such incidents to the DoDCAF Navy via JPAS or successor system, without applying adjudication.

2. In order to maintain a robust and continuous evaluation program the following responsibilities must be fulfilled:

a. Staff Judge Advocate. The Staff Judge Advocate (SJA) office will provide the Security Manager copies of the Officers Disciplinary Notebook (ODN), Non-judicial Punishments, Court-martials, and any other legal reports necessary to meet this reporting requirement.

b. Substance Abuse Control Officer. The Substance Abuse Control Officer will provide the Security Manager with a copy of the weekly substance abuse report.

c. Government Travel Charge Card Coordinator. The government travel charge card coordinator will provide the Security Manager a copy of the monthly Hierarchy Delinquency Report.

d. Provost Marshall's Office Police Blotter. MCB Quantico Provost Marshall's Office will provide the Security Manager a copy of the daily Police Blotter report.

e. Naval Criminal Investigation Services. Security Managers must create and maintain a working relationship with their resident Naval Criminal Investigation Services (NCIS) Special Agent. NCIS will provide the Security Manager many services to include, but not limited to, counterintelligence and insider threat briefs, PI notifications, and investigation reports, as applicable.

7001. Adverse Actions. In conjunction with reports made to the DoDCAF Navy via JPAS or successor system, the only other action a command may take is to suspend and individual's access to CNSI.

1. Only the DoDCAF Navy can take action on eligibility.

a. If this determination is made, DoDCAF Navy will issue the following notices to the command. All notices from DoDCAF Navy received on TECOM personnel will be handled by the Security Manager only. The Security Manager will follow all instructions provided to them within the notice.

(1) Letter of Intent (LOI) to Deny or Revoke.

(2) Letter of Denial (LOD).

b. Appealing a DoDCAF Navy decision. If DoDCAF Navy issues a LOD revoking or denying eligibility, all access to CNSI must be suspended via JPAS or successor system, and the individual must be removed from all sensitive duties. The LOD will contain instructions for the individual to appeal the DoDCAF Navy decision, along with reference (f).

2. In accordance with reference (f), military persons whose access to CNSI has been suspended for cause or eligibility for access has been revoked or denied by the DoDCAF Navy will not Permeant Change of Station or Assignment (PCS/A) until a final decision has been rendered regarding appeals of their case. The Security Manager will report all suspension and revocation actions to Manpower Management Enlisted Assignments (MMEA) or Manpower Management Officer Assignments (MMOA), as appropriate, and request PCS/A orders be held in abeyance pending resolution of the appeal.

CHAPTER 8

INDUSTRIAL SECURITY

8000. Basic Policy. The Security Manager, on behalf of the CG, is required to establish an Industrial Security Program if the command engages in classified procurement with U.S. Industry, educational institutions or other cleared U.S. entities, hereafter referred to as contractors. This chapter supplements regulations to ensure the CG meets his/her requirements outlined in references (c) through (f).

8001. Contracting Officer Security Representative. The CG will designate, in writing, a qualified security specialist as a Contracting Officer Security Representative (COSR). This appointment will be held by the Security Manager.

1. All designated COSRs are required to complete training within 30 days of assuming COSR responsibilities. Refer to reference (f) for training information.

2. The COSR is responsible for coordinating with program managers and technical and procurement officials during all phases of the procurement process to ensure security considerations are reviewed and implemented in compliance with established policy and to ensure the Statement of Work (SOW) and Contract Security Classification Specification (DD 254) are prepared properly.

3. The COSR will ensure all industrial security functions and requirements are accomplished when CNSI is provided to a contractor for performance on a classified contract.

4. For SCI contracts, the COSR will work with MCIA, directly.

8002. Classified Contracts

1. All contracts requiring classified work require a DD 254. The Security Manager will maintain a copy of all DD 254's for all contracts requiring classified work. The TECOM Security Manager functions as the COSR and handles all requirements for classified contracts.

a. All TECOM DD 254s must be signed by the COSR.

b. At no time will a DD 254 be accepted if found to be signed by a Facility Security Officer or someone other than a designated COSR.

c. In addition to the DD 254, the Security Manager will maintain copies of the associated SOW or Performance Work Statement (PWS).

2. All contracts must be annotated in the SOW/PWS all IT systems, applications, networks, and/or software required, with appropriate investigative requirements.

8003. Visit by Cleared DoD Contractors. Refer to references (c) and (f).

8004. Transmission or Transportation. Appropriately cleared and designated DoD Contractors may act as couriers, escorts or handcarriers for CNSI in accordance with Volume 3 of reference (a), and reference (c). The Security Manager will issue authorization letters to a contractor if and when they need to courier, escort or handcarry CNSI.

8005. Contract Support Public Trust Determinations. Refer to reference (f).

CHAPTER 9

Controlled Unclassified Information

9000. Basic Policy. CUI is information requiring safeguarding or dissemination controls pursuant to and consistent with law, regulations, or government policies in accordance with Volume 4 of reference (a), but does not meet the requirements for CNSI as required by Volume 1 of reference (a).

1. This chapter provides supplemental policy for the handling and protection of CUI within EDCOM as required by Volume 4 of reference (a).

2. All personnel are individually responsible for compliance with the requirements outlined in this chapter.

3. CUI must be identified and protected from unauthorized disclosure, appropriately designating, marking, safeguarding, disseminating, decontrolling, and destroying, information.

9001. Applicability

1. Policy, procedures, and minimum standards for safeguarding CUI are applicable to all EDCOM personnel, both military and civilian, to include cleared and uncleared contractor personnel working under the purview of the CG and contractors and consultants, assigned the requirements of this chapter via contract clauses.

2. Contractors and consultants requiring access to CUI shall be assigned the requirements within Volume 4 of reference (a) through appropriate contract clauses.

9002. Responsibility. The Security Manager will is responsible for the management of CUI and will be responsible for ensuring compliance with policies and procedures for identifying, marking, safeguarding, dissemination and destruction of CUI.

9003. Controls of CUI. Refer to Volume 4 of reference (a) for policy on identification, access, safeguarding, marking, decontrolling, and dissemination of CUI.

9004. Education and Training. All EDCOM personnel, military and civilians (to include cleared and uncleared contractors) will receive CUI education and training which provides knowledge of CUI. The training will be inclusive with the command's orientation, indoctrination and annual refresher training.

9005. Destruction of CUI. As required by Volume 4 of reference (a), CUI may be destroyed by any of the means approved for the destruction of CNSI or by any other means which would make it difficult to recognize or reconstruct the information. Contact the Security Manager for assistance prior to purchasing any shredders for the destruction of CUI.

9006. Dissemination of CUI to Foreign Nationals. U.S. CUI is disclosed to foreign nationals only in accordance with reference (k). At no time will any member of EDCOM, regardless of status, provide U.S. CUI to any foreign national without written approval from the EDCOM FDO.

DIRECTIVE NO.	DIRECTIVE TITLE (OR SHORT TITLE)	J	F	M	A	M	J	J	A	S	O	N	D
EDCOMO 5510.1	EDCOM INFO & PERSONNEL										[✓ O]		

DATE PROMULGATED	PROMULGATED BY	DISTRIBUTION	CLASSIFICATION
07 OCT 2019	SEC	A	UNCLASS.

DIRECTIVE REVIEW NAVMC 10974 (REV. 8-97))(EF) SN: 0109-LF-069-0400 (5215)

In accordance with current edition of MCO P5600.31, this directive has been reviewed for necessity, current applicability, and to assure consonance with existing law and with national and Department of Defense policy, by:

DIRECTIVE NUMBER	DATE REVIEWED	CANCELLED	CANCELLED BY	REMARKS (New, Revision, Change)	SIGNATURE OF REVIEWING OFFICER
5510.1	07 OCT 2019			NEW	
5500.1	17 JAN 2020			No change	
5510.1	5 DEC 2021			No Change	GySgt Quinonez

DIRECTIVE NO.	DATE CANCELLED	J	F	M	A	M	J	J	A	S	O	N	D