UNITED STATES MARINE CORPS
MARINE CORPS UNIVERSITY
EDUCATION COMMAND
2076 SOUTH STREET
QUANTICO, VIRGINIA 22134

5530
Sec

FEB 2 1 2019

MARINE CORPS UNIVERSITY/EDUCATION COMMAND ORDER 5530.1

From: Commanding General, Education Command
To: Distribution List

Subj: EDUCATION COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM STANDING OPERATING PROCEDURES FOR SECURE ROOMS

Ref: (a) MCO P5510.18A
(b) MCO P5530.14
(c) SECNAV M-5510.30
(d) SECNAV M-5510.36
(e) MCBO 5510.1C
(f) Education Command Emergency Action Plan
(g) CNO/USMC IA PUB 5239-22
(h) Education Command Security Instruction

Encl: (1) Education Command Standing Operating Procedures for Secure Rooms

1. Situation. This document establishes the Standing Operating Procedures (SOP) for Education Command personnel who work in or conduct work in the designated Secure Rooms (SR) rooms 1009, 2007, and 3182 in building 2044. This SOP also includes personnel who have access to classified material via SIPRNET clients inside the designated SR's office spaces rooms 1009, 2007, and 3182 in building 2044.

2. Mission. This SOP provides the guidelines and operational procedures for the use of the secure rooms located at Marine Corps University.

3. Execution. All Education Command military, government, and contractor personnel will review and follow the guidelines contained in this SOP and be familiar with the guidelines outlined within references (a) through (h).

4. Administration and Logistics. Recommended changes to this SOP are encouraged and should be submitted to Education Command via the Command Security Manager for review.

5. Command and Signal

a. Command. This Order is effective on the date signed.

b. Signal. This Order is applicable to all Education Command personnel.

6. Point of contact regarding this matter is Christopher Cabaniss at (703) 432-5578.

W. J. Bowers

W. J. BOWERS

Distribution List: A

TABLE OF CONTENTS

CHAPTER 1

SECURITY MANAGEMENT, ADMINISTRATION & EDUCATION

CHAPTER 1

SECURITY MANAGEMENT, ADMINISTRATION & EDUCATION

1000. SECURITY MANAGEMENT

1. The Commanding General, Vice Presidents, Directors, Staff, and members of Education Command are responsible for ensuring Department of the Navy and Marine Corps policies on personnel and physical security programs are properly instituted and maintained throughout Education Command. The effectiveness of the Education Command security program depends on a team of professionals working together to fulfill the Commanding General's responsibilities.

1001. SECURITY ADMINISTRATION

1. All personnel are required to check in with the Education Command Security Manager. All military and civilian personnel will be assigned a billet identification code, conduct annual security training, have security clearance verified, sign an SF-312 and have the need to know before access is granted to classified material.

2. To obtain a Secret Internet Protocol Router Network (SIPRNet) account, Education Command personnel must complete a DD2875 System Authorization Access Request (SAAR) form, a SIPRNet Account Request form and a Statement of Understanding (SOU), available from the Education Command Information Technology (IT) Section, a current Cyber Awareness Training (CYBERM000) certificate available at www.MarineNet.usmc.mil and a Derivative Classification training certificate (Renewed every two years). SIPRNet accounts will not be authorized without completing all the required forms, which must be signed by a supervisor, Staff Non-commissioned Officer or above and the Education Command Security Manager. A Secret/Top Secret clearance and Northern Atlantic Treaty Organization brief are required to obtain a SIPRNet account.

3. Information Technology (IT) Designations. IT Designations will be made for all Education Command Headquarters personnel. IT Designations are made based on input from the Security Manager, EDCOM Information Systems Security Manager (ISSM), position descriptions, statements of work, Billet Identification Code classification, and additional duties. IT designations for contractors will be made based on the DD 254s. Per Enterprise Cybersecurity Manual (ECSM) 007, filling out the IT designation on the SAAR is the responsibility of the supervisor.

4. Check-out. The following steps will be taken when an Education Command member (military, government civilian, or contractor) checks out of Education Command:

a. If the member had access to any safes, the combinations to the external X-09/10 combination locks within Education Command will be changed immediately upon the member's departure.

CHAPTER 1

SECURITY MANAGEMENT, ADMINISTRATION & EDUCATION

1000. SECURITY MANAGEMENT

1. The Commanding General, Vice President's, Directors, Staff, and members of Education Command are responsible for ensuring Department of the Navy and Marine Corps policies on personnel and physical security programs are properly instituted and maintained throughout Education Command. The effectiveness of the Education Command security program depends on a team of professionals working together to fulfill the Commanding General's responsibilities.

1001. SECURITY ADMINISTRATION

1. All personnel are required to check in with the Education Command Security Manager. All military and civilian personnel will be assigned a billet identification code, conduct annual security training, have security clearance verified, sign an SF-312 and have the need to know before access is granted to classified material.

2. To obtain a Secret Internet Protocol Router Network (SIPRNet) account, Education Command personnel must complete a DD2875 System Authorization Access Request (SAAR) form, a SIPRNet Account Request form and a Statement of Understanding (SOU), available from the Education Command Information Technology (IT) Section, a current Cyber Awareness Training (CYBERM000) certificate available at www.MarineNet.usmc.mil and a Derivative Classification training certificate (Renewed every two years). SIPRNet accounts will not be authorized without completing all the required forms, which must be signed by a supervisor, Staff Non-commissioned Officer or above and the Education Command Security Manager. A Secret/Top Secret clearance and Northern Atlantic Treaty Organization brief are required to obtain a SIPRNet account.

3. Information Technology (IT) Designations. IT Designations will be made for all Education Command Headquarters' personnel. IT Designations are made based on input from the Security Manager, EDCOM Information Systems Security Manager (ISSM), position descriptions, statements of work, Billet Identification Code classification, and additional duties. IT designations for contractors will be made based on the DD 254s. Per Enterprise Cybersecurity Manual (ECSM) 007, filling out the IT designation on the SAAR is the responsibility of the supervisor.

4. Check-out. The following steps will be taken when an Education Command member (military, government civilian, or contractor) checks out of Education Command:

a. If the member had access to any safes, the combinations to the external X-09/10 combination locks within Education Command will be changed immediately upon the member's departure.

b. All access control rosters will be modified.

1002. SECURITY TRAINING

1. The purpose of the Education Command Security Training Program is to ensure that all personnel assigned to Education Command understand the need to protect sensitive and classified information and remain current on annual Marine Corps security training requirements.

2. All Education Command military, government civilian and contractor personnel, with access to classified information, must receive/complete the following annual brief/training:

a. Derivative Classifier Training. This training will be completed upon initial entry into the organization and then once every two years. This training suffices as written procedures for how to mark classified documents correctly. Classifiers shall be trained and recertified by Education Command Security every two years.

b. SIPRNet Security Education. Use the link below to complete the on-line SIPRNet security training:

https://ehqmc.usmc.mil/org/mccdc/TECOM/genstaff/G-6/ITSS/IA/Information%20Assurance%20Library/Forms/AllItems.aspx?RootFolder=%2forg%2fmccdc%2fTECOM%2fgenstaff%2fG%2d6%2fITSS%2fIA%2fInformation%20Assurance%20Library%2fTECOM&FolderCTID=&View=%7bA802F589%2dDDD1%2d4480%2dA8ED%2dB36CD66FA576%7d

c. Counter Intelligence Briefing conducted by the Naval Criminal Investigative Service (NCIS) at Quantico, Virginia.

d. Security Refresher Training.

3. Any deviation to the rules provided within this SOP or any other security principle should be reported to the Education Command Security Manager immediately.

4. If classified documents are found in an unprotected or unsecure fashion they should be secured immediately and the Education Command Security Office should be notified.

1003. SECURITY RESPONSIBILITIES

1. The Education Command Security Manager will appoint Security Representatives in writing.

2. The appointed Security Representatives will assume daily responsibilities of the SR's. The Security Representatives duties include:

a. Keeping a log book of all SIPR asset issuances.

b. Disarming and arming the Intrusion Detection Systems (IDS).

c. Completing the end of day checklist (SF-701) and the Security Container Check Sheet (SF-702).

d. Maintaining access control log books.

CHAPTER 2

PHYSICAL SECURITY

CHAPTER 2

PHYSICAL SECURITY

2000. PHYSICAL SECURITY

1. The Education Command Security Manager (SM) is responsible to the Commanding General concerning the adequacy of the physical security posture within the Education Command Area of Responsibility (AOR). He/she will perform quarterly security assessments identifying any vulnerability and taking appropriate corrective action. The SM is responsible for ensuring:

a. Compliance with Marine Corps Base Quantico physical security policy and procedures set forth by reference (e).

b. Access to classified information is limited and controlled within authorized spaces to those with the required security access and need to know.

c. The Education Command Emergency Action Plan reference (f) complies with Education Command Standard Operating Procedures.

d. Physical security measures are implemented to safeguard the Education Command AOR.

2001. VISITOR CONTROL

1. All Education Command personnel are responsible for visitor escorts for meetings and/or training in and around the Education Command Secure Rooms (SR's). All personnel who are not on the Education Command access roster should be deemed an un-cleared visitor and escorted at all times. Their presence should be announced when entering SR's.

2. All visitors to Education Command that require access to classified material are required to submit a visit request via JPAS through their security office to SMO Code MS3302, that includes a point of contact (POC), POC telephone number, dates of visit and level of access required.

2002. SECURE ROOMS (SR)

1. The following locations are designated as Secure Rooms in Education Command:

Building: 2044 Rooms 1009, 2007, and 3182.

2. The following rules apply to SRs:

a. Permanent personnel assigned to the designated SRs will ensure, through the Education Command SM and JPAS, that they are on the Education Command (SMO MS3302) access roster. These personnel shall also meet the annual security training requirements. All Education Command personnel that are granted access to the SRs will report to the Provost Marshalls Office (PMO) to have their Common Access Card (CAC) coded for the prescribed SR access control point.

b. When classified material is to be accessed or viewed, all personal electronic devices (PED) to include but not limited to smartwatches, iPads, cellphones, laptops and iPods shall be left outside the SRs.

c. When classified material is being processed, an "open" placard is to be placed outside the hatch indicating that classified material is currently being processed by personnel in the office space and access to the office space is currently restricted to those with access.

d. Workstations processing classified material, and due to the desk configuration, cannot maneuver a computer monitor out of common view, shall have a privacy screen attached.

e. Unclassified workstations occupying the same desk space as those with classified workstations shall maintain a minimum 40" separation between computing assets.

f. Cleaning crews and other non-cleared personnel are not authorized in these office spaces while classified material is being processed.

g. Classified material will never be left unattended. When not in use, ALL classified material will be secured in the GSA safe within SRs.

h. SIPR tokens will never be left unattended and remain in the custody of the issuant.

i. Monitors will be turned off when un-cleared personnel are present.

j. It is the appointed security representative's responsibility for hanging placards on all SRs.

3. GSA approved safes will only reside within approved SRs.

4. Special precautions must be taken regarding classified discussions within the SRs.

2003. KEY CONTROL. All non-assigned hard keys will be stored in a GSA approved safe in MCU G-1 office.

2004. PHYSICAL SECURITY CHECKS

1. Education Command Security Representatives who have been appropriately trained by the Education Command Security Manager, will check the SIPR conduit daily along with the safe containing the SIPR switch and encryption device.

2. It is the responsibility of all personnel who access GSA approved safes to fill out the adjacent Standard Form SF-702s each and every time they are opened and secured.

3. Education Command Security Representatives will check all safes to ensure that they are secured along with initialing the "Checked By" column for all SF-702s. At the conclusion of all GSA safes being checked in building 2044, the Education Command security point of contact will complete a standard form SF-701, which is the end of the day checklist for the SR. In the absence of Education Command security point of contact, the last person with access to the SR will be responsible for the end of the day checklist.

4. It is the responsibility of the Education Command representative or the designated Education Command Security point of contact to ensure that these forms are being filled out correctly. Quarterly inspections will be completed and the results supplied to the Education Command Security Manager.

CHAPTER 3

MARKING, STORAGE, AND COURIERING OF CLASSIFIED MATERIAL

CHAPTER 3

MARKING OF CLASSIFIED MATERIAL

3000. MARKING OF CLASSIFIED MATERIAL

1. Document Cover Sheets. Classified document cover sheets are available at the Education Command Security Office.

a. Secret Cover Sheet, SF-704 (NSN 7540-01-213-7902)

b. Confidential Cover Sheet, SF-705 (NSN 7540-01-213-7903)

c. Unless the document is clearly marked unclassified at the top and the bottom, all documents will use one of the coversheets above.

2. Colored Paper. All documents printed off of the SIPRNET will be printed with pink paper.

3. The originator is responsible for marking classified "Working Papers", such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain classified information, as follows:

a. Conspicuously marked centered top and bottom of each page with the highest overall classification level of any information they contain.

b. Marked as "Working Papers" on the top left of the first page in letters larger than the text.

c. Date when created

d. Name of the individual who created the "Working Papers".

e. Section of the individual who created the "Working Papers".

f. Destroy before 180 days or Control (assigned a control number and added to classified inventory).

4. The originator will also ensure the "Working Papers" are destroyed immediately after use and/or not maintained for longer than 180 days. If "Working Papers" are maintained longer than 180 days, they are assigned a control number and added to classified inventory by the Education Command Security Manager. Under no circumstances will the "Working Papers" leave MCB, Quantico. The Security Manager will enforce this policy by conducting random inspections of classified materials.

5. All classified "Working Papers" when created are placed in the binders in the safe labeled "Working Papers." The binders are marked for classified material only.

6. All pink paper or classified paperwork if marked "Working Papers" will be shredded in the GSA approved shredder with in the SR when no longer needed. All media and all classified material with a control number placed on it, will be destroyed by the Education Command Security Office and logged in the destruction log book.

3001. STORAGE OF CLASSIFED MATERIAL AND MANAGEMENT OF CLASSIFIED STORGE CONTAINERS

1. Classified material will be stored in a GSA approved security container when not in use by cleared Education Command personnel.

2. Education Command Security Representatives are responsible for submitting the security container combinations to the Education Command Security Office. The container combination is submitted using a SF-700, security container information envelope. The information on the SF-700 must be neatly printed with no strikeovers (mistakes). The SF-700 lists the name, home address and home phone number of all personnel who know the combination for the security container. In addition, REQUIRED information includes: post, building, room number, activity, container number, class of container, lock model, date combination changed, and name of person making the change. The classification level will be printed at the top of the SF-700. Remove the front portion of the envelope and tape to the inside drawer of the security container.

3. Combinations are changed when:

a. First placed in use.

b. An individual knowing the combination no longer requires access.

c. Subjected to compromise.

d. Taken out of service.

e. Annually

4. The Friday before the Christmas federal holiday will be designated as a clean out day for Education Command. All paperwork that is not needed for the mission or historical purposes will be shredded or destroyed as appropriate.

3002. COURIERING OF CLASSIFIED MATERIAL

1. Couriers of classified material will be issued a courier card or courier letter designating that they have been briefed and are aware of their responsibilities as couriers of classified material.

2. Courier cards and letters will be issued by the Education Command SM in accordance with the Education Command Security Instruction.

DIRECTIVE NO. EDCOMO 5530.1	DIRECTIVE TITLE (OR SHORT TITLE) SOP FOR SECURE ROOMS	J [✓ F] M A M J J A S O N D
DATE PROMULGATED 21 FEB 2019	PROMULGATED BY SEC	DISTRIBUTION A
CLASSIFICATION 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
5530.1	21 FEB 2019			NEW	
5530.1	21 FEB 2020			No CHANGE	GySgt Pulliam
5530.1	2 DEC 2021			Revision	GySgt [illegible]

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

Designed using FormFlow 2.15, HQMC/ARAE, Apr 98