UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NORTH CAROLINA 28542-0080

II MEFO
5500.1A
G-2/SSO
MAY 06 2019

II MARINE EXPEDITIONARY FORCE ORDER 5500.1A

From: Commanding General, II Marine Expeditionary Force
To: Distribution List

Subj: II MARINE EXPEDITIONARY FORCE SPECIAL SECURITY OFFICE STANDARD OPERATING PROCEDURE (SHORT TITLE: II MEF SSO SOP)

Ref: (a) ICD 705
(b) DODM 5105.21
(c) MCO 5530.15
(d) DODM 5105.21
(e) ICD 704
(f) ICD 710
(g) DIAM 50-4
(h) DIAM 50-24
(i) SECNAVINST 5510.30B
(j) SECNAVINST 5510.36A
(k) SECNAVINST 5329.19
(l) MCO 1200.17A, MOS Manual
(m) AMHS Message, DTG 101326Z Jun 11, Personnel Security Investigations

Encl: (1) II MEF SSO SOP

1. Situation. The Special Security Office (SSO) provides a reliable and secure means to receive and disseminate Sensitive Compartmented Information (SCI) to authorized recipients within the II Marine Expeditionary Force (II MEF) and external government and military organizations.

2. Cancellation. II MEFO 5500.1

3. Mission. The procedures set forth in this Order implement the references as they pertain to this command and establish the II MEF SSO Standard Operating Procedures.

4. Execution. All personnel indoctrinated into SCI will become familiar with and adhere to the procedures contained in the enclosures.

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

5. Administration and Logistics. Submit all recommendations concerning this Order to the II MEF SSO.

6. Command and Signal.

a. Command. This Order is applicable to all II MEF units.

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

7. The point of contact for this matter is the II MEF SSO at 910-451-8279.

R. F. HEDELUND

DISTRIBUTION: A

TABLE OF CONTENTS

CHAPTER 1
GENERAL

1-1. POLICY AND GUIDANCE. The policies and regulations governing the operation of the II MEF SCIF are promulgated by various agencies and commands within the Department of Defense Intelligence Community. Below is a partial list of those agencies and commands:

a. DNI . . . . . Director, National Intelligence
b. DIRNSA. . . . . Director, National Security Agency
c. DIA . . . . . Defense Intelligence Agency
d. CNO . . . . . Chief of Naval Operations
e. ONI . . . . . Office of Naval Intelligence
f. CMC . . . . . Commandant of the Marine Corps
g. COMMARFORCOM. . Commander, Marine Corps Forces Command
h. CG II MEF . . . Commanding General, II Marine Expeditionary Force

1-2. REFERENCE MATERIALS. The following is a list of the primary sources of information regarding the operation of the II MEF SCIF:

a. ICD 705, Sensitive Compartmented Information Facilities

b. IC Tech Spec for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

c. DOD C 5105.21 NavSupp Mar 97, Navy Department Supplement, Sensitive Compartmented Information Security Manual for Administrative Security

d. MCO 5530.15, Marine Corps Physical Security Manual

e. DOD S 5105.21-M-1 Mar 95, Sensitive Compartmented Information (SCI) Security Manual

f. ICD 704, Personnel Security Standards and Procedures Governing Eligibility for access to Sensitive Compartmented Information

g. ICD 710, Authorized Classification and Control Markings Register

h. DIAM 50-4, Security of Compartmented Computer Operations

i. OPNAVINST 5510-30A, The Department of the Navy Personnel Security Program for access to Classified Information

j. OPNAVINST 5510.36, The Department of the Navy Information Security Program for classification, safeguarding, transmission and destruction of classified material

k. Joint DODIIS/Cryptologic SCI Information Systems Security Standards

l. MCO 1200.17a, MOS Manual

m. AMHS Message, DTG 101326z Jun 11, Personnel Security Investigations

CHAPTER 2
PHYSICAL SECURITY

2-1. GENERAL. Reference (a) is considered the "bible" for physical security. It establishes the minimum standards for physical security criteria of SCIFs. Reference (b) provides specific guidance for physical security for SCIFs within the Department of the Navy.

2-2. THE SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF). The II MEF SCIF located in Wallace Creek Building 504 (WC504) is a SCIF housing elements of the II MAGTF INTELLIGENCE CENTER (MIC), II MEF G-2, Second Marine Division, 2D Marine Expeditionary Brigade, II Marine Information Group, 2D Intelligence Battalion, 8th Communications Battalion, 2D Marine Logistic Group, and the National Geospatial Agency Liaison. The II MEF SCIF located in H-1 Wing 1H South (1HS) is occupied by the II MEF G-2, II MEF G-35, II MEF G-3 STO. Both SCIFs are accredited as SCI Part-Time Operations Facilities. All offices must be closed at night, checked at the end of the day by the person securing the SCIF. A locked door within the SCIF does not constitute an additional security device, nor does it take the place of a cleared escort when access by un-cleared personnel is necessary, instead it serves as an administrative control. In addition, II MEF policy requires that all lights, fans, computer screens, and other electronic devices be logged off of or powered down after working hours.

a. SECURITY DUTIES. Each unit working in WC-504 is required to share the responsibility of SSO/Security for WC-504; II MEF SSO is responsible for coordinating the monthly list of personnel that will fulfill the SSO/Security responsibilities and distribute it to those applicable units. Each unit (to include but not limited to II Marine Information Group, Second Marine Division, 2D Marine Logistics Group, 2D Marine Expeditionary Brigade, 8th Communications Battalion, 2D Intelligence Battalion…)will contribute at least 1 Marine via Temporary Assigned Duty (TAD) to II MEF G2 in support of this SSO/Security responsibility. Those SSO/Security responsibilities include but are not limited to: opening & closing of the SCIF, providing personnel for the entry control point (ECP) duty for the SCIF, providing SSR personnel to support the SCIFs day to day operations, etc. Additionally, the security duties are outlined in the ECP SOP.(see Appendix AC)

2-3. OPEN/CLOSE PROCEDURES. Normal working hours of the II MEF SCIFs will be 0600-1730 Monday through Friday. Personnel that are authorized to open and close the SCIFs will be issued a Personal Identification Number (PIN) for the Intrusion Detection System (IDS) and will be given the combination for the SCIF X-09 or X-10 by the II MEF SSO. At the time that the door combination is issued the SSO will conduct training with the individual in order to ensure that they understand the proper operation of all systems.

a. OPEN. During normal operations, when a II MEF SCIF is opened, the SF-702 will be filled out by the person that opens the SCIF. For after-hours or weekend/holiday openings, the sections requiring access are required to have an authorized person (within that section) conduct the opening. The person opening the SCIF after-hours is required to remain in the SCIF until all work is complete; at which time they will lock the SCIF. Every section requiring entry will gain authorization from the SSO Chief before opening the SCIF outside of normal working hours. The MEF SSO is not required to provide personnel to open or close for SCIF tenants outside of normal working hours. Each tenant unit is required to have designated personnel to fulfill this function.

b. CLOSE. During normal operations the SCIFs will be closed at 1730. Both II MEF SCIFs will only be closed by a member of the Open/Close Roster for that SCIF. The person conducting the closing will physically check each office in the SCIF and all heads to ensure that no one else is in the SCIF. Once the SCIF is clear of all personnel, the IDS will be set using the issued PIN and the main hatch will be locked with the X-09 or X-10. Both the SF-702 and SF-701 will be completed by the person conducting the closing. After hours weekend/holiday closing will be completed by the same person that opened the SCIF.

2-4. INTRUSION DETECTION SYSTEM. The Intrusion Detection System (IDS) will be armed **anytime** the SCIF is unmanned. The IDS is maintained by contract personnel through PMO and utilizes the same Local Area Network (LAN) as the automated access control. Reference (b) requires that the IDS be tested semi-annually; this requirement is included in the Memorandum of Agreement (MOA) that has been established between the Commanding General, II Marine Expeditionary Force and Commanding Officer, Marine Corps Base Camp Lejeune. The SSO Chief will coordinate testing with PMO physical security anytime during the first and third quarter of each calendar year. The tests will be stored in the SCIF binder.

a. PMO RESPONSE TO IDS ACTIVATION. PMO will respond to all activation of the SCIF IDS within 15 minutes as established in the MOA and as required by references (a) and (c). When PMO responds to an IDS activation the PMO Desk Sergeant will contact an SSO representative via phone. The SSO representative will go to the SCIF entry point to coordinate with onsite PMO officers within 60 minutes of being contacted. The SSO representative will identify themselves to the onsite PMO officers and provide their military ID to the officer to verify their identity. If no forced entry is suspected the SSO representative will conduct a walkthrough of the SCIF, accompanied by one PMO officer, to ensure that no unauthorized access or compromise has occurred. Once the SCIF is found to be clear, the SSO representative will arm the IDS and secure the front hatch utilizing the X-09 or X-10. If the SSO representative is not the SSO Chief, then the SSO Chief will be contacted and briefed on

the situation. The IDS activation will be reported to the DAC/S G-2 no later than 0730 on the next working day.

1. If evidence of forced entry is noted, the SSO representative will allow PMO officers to enter and clear the SCIF. The SSO representative will facilitate entry into any locked areas with the exception of the STO office. The STO is secured by an X-09. If no evidence of forced entry of the STO room is observed then PMO will not be admitted. The STO Chief will be contacted to verify that the STO is secure. Once the SCIF is cleared of any intruders, the forced entry will be reported immediately through the SSO chain-of-command to the DAC/S G-2 and AC/S G-2.

2. Bi-annual testing of the response force is required by reference (b) and is established in the MOA. The SSO Chief will coordinate with PMO physical security twice per calendar year to have a full PMO response force exercise conducted. If PMO units do not respond within 15 min, the test will not be considered successful and an additional test will be required. The test results will be recorded in the administration file cabinet.

2-5. TWO-PERSON RULE. In accordance with reference (d), two-person integrity is no longer required for SCIF operations. Two-person integrity will continue to be maintained on cryptologic keying material (keymat). Keying material will be secured in a GSA approved two combination safe. Each individual having access to the safe will have knowledge of only one combination. Two persons must be present at all times while the safe is open and anytime keymat is in use, or outside of a locked safe. In cases where one person will be present all keymat must be properly secured. The security container check sheet, SF 702, will be properly annotated each time the safe is opened or closed.

2-6. ACCESS CONTROL. SCIF badges will be issued to identify the status of personnel within the SCIF. Badges will be clearly visible, worn above the waist and displayed at all times while within the SCIF. Badges will be removed immediately upon exiting buildings H-1 or WC504. Specific instructions for SCIF access are listed below. Access control policy is the responsibility of the SSO and SSO personnel, all personnel working within the SCIF are responsible for enforcement of the access control policy. Any requirement for after-hours access must be coordinated with the SSO Chief.

a. ROUTINE ACCESS. Routine access to the SCIF is limited to those personnel that work in the SCIF at least two days a week. This will include all indoctrinated personnel that are designated to require constant access to the II MEF SCIF by the SSO Chief. These personnel are issued an ID badge and given an individual access number. These hours will be Monday thru Friday 0700 to 1730. Those authorized to open/close the SCIF will be issued badges with unrestricted access

(24 hrs a day, 7 days a week). The only personnel authorized to grant after-hours access are the AC/S G-2, DAC/S G-2, SSO and SSO Chief. **Loss of or damage to this card, or compromise of the individual access number must be reported to the SSO immediately. The access badge will be turned into the SSO before indoctrinated personnel execute permanent change of station (PCS) orders, when SCIF access is no longer required or when requested by SSO or appropriate II MEF G-2 personnel.**

1. VISITOR ACCESS. An access roster of all SCI indoctrinated personnel that require access to a II MEF SCIF will be maintained at each SCIF entry point. This access roster will also contain all current visit and permanent certifications. Indoctrinated individuals requiring access to the SCIF must present a valid Common Access Card (CAC) to verify information on the Access Roster. **All visitors must have a valid need-to-know.** All visitors will sign the visitor log located in the SSO office when they enter and exit the SCIF. A badge must be worn by all personnel inside the SCIF, whether they are cleared or un-cleared. This badge must be worn above the waist and be clearly visible at all times. An identification card will be traded with the II MEF SSO for a temporary SCIF badge.

a. Un-cleared individuals requiring access to the SCIF will be admitted on a case by case basis for official business only. **For un-cleared personnel, routine administrative business WILL NOT be conducted in the SCIF; this includes weigh-ins, NJPs, counseling, etc.** Prior to entry, all offices within the SCIF will be notified that un-cleared personnel will be on deck by placing appropriate signs on the SCIF entry door and turning on the un-cleared visitor light. Each area the individual will enter must be sanitized of classified material prior to entrance. All other areas will be secured from visual observation. The individual will then be allowed access and must be escorted at all times for the duration of their stay within the SCIF. Escorts are only required for un-cleared personnel and will be assigned by the sponsoring office. Escorts will be issued an escort badge and receive a brief of their responsibilities prior to being allowed to escort un-cleared individuals.

2. ACCESS BY EMERGENCY PERSONNEL. In emergency situations un-cleared emergency personnel will be allowed immediate access and will not be made to remove any equipment (e.g. side-arm, radios). Escorts for emergency personnel will be provided when feasible. An Inadvertent Disclosure Form will be filled out by emergency personnel prior to their departure from the II MEF SCIF if it does not interfere with their duties. **At no time will emergency personnel be made to complete an inadvertent disclosure form if it would put any person at risk of life or limb.** In situations that emergency personnel cannot complete the inadvertent disclosure form prior to exiting the SCIF the SSO office will follow-up with the agency or department involved to arrange the

completion of required forms. An example of this form is located in Appendix A.

2-7. EMERGENCY ACTION PLAN. Physical security measures are established to prevent unauthorized access to classified and cryptographic information during emergency situations. The possibility of unauthorized access is increased during times of emergency. An Emergency Action Plan (EAP) detailing specific guidelines has been published and is located in each office. The II MEF SCIF EAP is located in Appendix B. The EAP must be tested annually to ensure all personnel are aware and capable of completing their required tasks. The extent of the test will be under the discretion of the SSO. In accordance with reference (a) the EAP must be reviewed and approved by the SIO annually, this review will be recorded on the master EAP located in the Administration file cabinet.

CHAPTER 3
SECURITY AWARENESS/EDUCATION

3-1. SECURITY AWARENESS/EDUCATION. In accordance with reference (e) all individuals nominated for or holding SCI access approval will be notified initially and annually thereafter of their responsibility to report to their cognizant security officers any activities or conduct that could conflict with their ability to protect classified information from unauthorized disclosure. The security awareness program is divided into three parts; initial indoctrination, periodic awareness enhancements, and debriefing.

a. Initial Indoctrination. Upon indoctrination, personnel will receive an initial security awareness brief that includes:

1. The need for and purpose of SCI material, and the adverse effect on national security that could result from its unauthorized disclosure.

2. The intelligence mission of the unit assigned, to include the reason the intelligence information is sensitive.

3. The administrative, personnel, physical, and other procedural security requirements of II MEF and those requirements peculiar to specific duty assignments, including information on who to consult to determine if particular outside employment or activities might be of concern.

4. Individual classification management responsibilities as set forth in appropriate references and regulation to include classification/declassification guidelines and marking requirements.

5. The definitions and criminal penalties for espionage, including harboring or concealing persons; gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797 and 798), the Internal Security Act of 1950 (Title 50, U.S.C., Section 783), the Intelligence Identities Protection Act of 1982 (Title 50, U.S.C., Sections 421 through 426).

6. The punitive and administrative sanctions for violation of or disregard for security procedures.

7. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

8. Individual security responsibilities including:

a. The prohibitions against discussing SCI in a non-secure area, over a non-secure telephone, or in any other manner that permits access by unauthorized persons.

b. The need to determine, before disseminating SCI, that the prospective recipient has the proper security access approval, the access needed in order to perform official duties, and that the recipient can properly protect the information.

c. The need to exercise security in activities as members of professional, commercial, scholarly or advocacy organizations that publish or discuss information on intelligence, defense or foreign affairs.

d. The continuing obligation to submit for review any planned articles, books, speeches or public statements that contain or purport to contain SCI or information relating to or derived from SCI, as specified by the nondisclosure agreements.

e. Obligation to report attempts (including blackmail, coercion and harassment) by unauthorized persons to obtain national security information, physical security deficiencies, and loss or possible compromise of SCI material.

f. Obligation to report to the SSO all activities or conduct of an individual who has access to SCI which relates to guidelines contained in reference (e).

g. Obligation to report involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.

h. Obligation to report foreign influence concerns/close personal association with foreign nationals.

i. Obligation to report sexual behavior that is criminal or reflects a lack of judgment or discretion.

j. Obligation to report unwillingness to comply with rules and regulations or to cooperate with security processes.

k. Obligation to report unexplained affluence or excessive indebtedness.

l. Obligation to report alcohol abuse.

m. Obligation to report illegal or improper drug use/involvement.

n. Obligation to report apparent mental or emotional disorder(s).

o. Obligation to report criminal conduct.

p. Obligation to report noncompliance with security requirements.

q. Obligation to report engagement in outside activities which could cause a conflict of interest.

r. Obligation to report misuse of information technology systems.

9. Identification of personnel by name and billet to which matters of security interest are to be addressed.

b. Periodic Awareness Enhancement. The SSO office must establish and maintain a continuous security awareness program that will provide frequent exposure to security awareness material. This may include live briefs, audiovisual presentations, printed material, or a combination thereof. The program is designed to meet the needs of II MEF as follows:

1. II MEF SSO has hung security awareness material throughout the SCIF area, to include the main hall, male and female head, and each office.

2. Appendix C contains a hard copy of the presentation used for the annual all hands security awareness brief. This presentation includes:

a. The current foreign intelligence threat for Jacksonville, North Carolina. This assessment is classified and filed in the physical security folder located in the SSO Chief's safe.

b. Current technical threat to the II MEF SCIFs.

c. Administrative, personnel, physical and procedural security requirements for those assigned or permitted access to the II MEF SCIF.

d. Individual classification management responsibilities.

e. Criminal penalties and administrative sanctions.

f. Individual security responsibilities.

c. Debriefing. When an individual is debriefed, final instructions and guidelines will be provided. This is to include:

1. The individual will read the appropriate sections of Title 18 and 50, U.S.C., with the intent that the criminal sanctions of the laws relative to espionage and unauthorized disclosure be clarified.

2. The continuing obligation, under the prepublication and other provisions of the nondisclosure agreement for SCI, never to divulge; publish; or reveal by writing, word, conduct, or otherwise, to any unauthorized persons any SCI, without the written consent of appropriate department/agency officials.

3. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation any attempt by unauthorized person to solicit national security information.

4. An acknowledgement that the individual no longer possesses any documents or material containing SCI.

5. A reminder of the risks associated with foreign travel and foreign association.

6. All elements above are included in the II MEF debrief (appendix D).

3-2. FOREIGN TRAVEL/CONTACTS. Personnel granted SCI access that plan official or unofficial foreign travel will report anticipated travel to the II MEF SSO and their immediate supervisor.

a. Supervisors will review the itinerary from a safety point-of-view.

b. The SSO will conduct a foreign travel brief to include:

1. A defensive travel security briefing or risk-of-capture brief.

a. A defensive travel security briefing alerts personnel to the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity. These briefings include courses of action to mitigate adverse security and personal consequences. The briefings also suggest passive and active measures to avoid becoming targets or inadvertent victims.

b. Risk-of-capture briefing alerts personnel of techniques used to force or trick them to divulge classified information if captured or detained and offers suggested courses of action to avoid or limit such divulgence.

2. A current Defense Intelligence Agency (DIA) threat assessment of each country to be visited. Threat briefs will include foreign intelligence services, terrorist or narcotic groups, indigenous

groups active in promoting insurgency, war, civil disturbance, or other acts of aggression.

c. Within ten days of return the individual will return to the SSO to complete a Foreign Contact Questionnaire (Appendix N) and report any suspicious activity.

CHAPTER 4
INFORMATION SECURITY

4-1. GENERAL. Every individual with access to classified material is responsible for safeguarding that material. The SSO's primary responsibility is to ensure the security of SCI and the continued eligibility of those that handle it. This involves providing guidance, awareness and education of the proper handling of SCI information. The SSO must ensure they are cognizant in all aspects of handling and safeguarding of SCI materials.

4-2. RESPONSIBILITIES. The author or drafter of classified material is responsible for properly complying with established security classification guidance and for properly applying that guidance to a document, including all security markings required for its protection, control and dissemination. All personnel who produce, transmit, reproduce, or extract SCI from documents or other material must ensure that the resulting SCI product is properly marked and protected. All SCI documents will be marked with the appropriate classification markings established by reference (f).

a. STANDARD CLASSIFICATION MARKINGS. Standard classification markings are markings that indicate the classification of a document, the authority for classification, and the declassification instructions.

1. Security classification markings are TOP SECRET, SECRET, and CONFIDENTIAL. The overall security classification and SCI notations will be conspicuously marked or stamped in letters larger and bolder than the text.

2. The classification authority designates the basis for classification and is an original classification authority for SCI. All classification decisions must be made in accordance with the appropriate classification guide.

3. Derivative classification is the incorporation, para-phrasing, re-statement or generation of information in a new form which is already classified, or the classification of information based on a classification guide from an original classification authority for SCI. Almost all SCI is derivatively classified from a classification guide. The classification guide or source document title or short title is cited as the authority in the classification authority line. When a document is classified by more than one source, the term "Multiple Sources" is placed on the classification authority line. A listing of the sources will be retained with the record copy of the document. When classification is based on a source document which states "Multiple Sources" as its authority, cite the document itself and not "Multiple Sources" as the classification authority.

b. SCI CONTROL SYSTEM MARKINGS. SCI materials will be marked with applicable SCI control system caveat(s) at the bottom of each page of a hardcopy document including the front and back covers. Place the caveat(s) immediately below the classification, centered on the bottom of the page. Use authorized abbreviations to mark portions.

1. If the material is to be controlled in only one SCI control system, mark the material HANDLE VIA (name of SCI control system) CONTROL CHANNELS ONLY.

2. If the material is to be controlled in two or more systems, mark the material HANDLE VIA (names of SCI control systems) CONTROL CHANNELS JOINTLY.

   a. CONTROL PROCEDURES. SCI documents and SCI channel materials will be individually accounted for during various stages of handling from the time of receipt through destruction. Procedures at this SSO involve logging material as it is received through the Defense Courier Service (DCS).

   b. CODEWORDS AND OPERATIONAL PROGRAM DESIGNATORS. SCI code words or operational program designators will be applied immediately following the security classification at the top and bottom of each page containing information requiring such protection. SCI codewords will be in letters larger and bolder than the text. When used in portion marking authorized abbreviations will be used.

3. Many SCI code words have been retired. Classification authorities must ensure they are using the most current classification guide when classifying a document.

4. SCI codewords and caveats are unclassified. Other code words are unclassified when standing alone. "Standing alone" is defined as completely disassociated from any substantive intelligence operation, national security policy, security classification, or related security matter. When these codewords or handling caveats are associated with intelligence activities, they are classified a minimum of CONFIDENTIAL. When used in conjunction with information about intelligence planning, collection, processing, dissemination, capabilities, relationships and the like, they require compartmented protection because of the association.

5. Digraphs and trigraphs are normally unclassified but should only be disclosed to personnel who understand the sensitivity and requirement for appropriate protection of the function. Authorized digraphs and trigraphs are found in the appropriate SCI control system manual.

c. DISSEMINATION CONTROL MARKINGS. SCI documents will be marked with the dissemination control markings prescribed in ICD 710. Show the

control markings on the title page, front cover, and at the bottom of each interior page. The long form on the dissemination control marking will appear once at the bottom of the title page and front cover. They will incorporate in the text of electronic communications, shown on graphics, and associated with data stored or processed in automated information systems. Include the dissemination control marking indicated by parenthetical use of marking abbreviations in portion markings at the beginning of appropriate portions.

4-3. MARKING SCI DOCUMENTS. Mark SCI documents as follows:

a. Front Cover

1. Highest classification of document (top and bottom centered)

2. SCI system caveat; dissemination control markings, special caveats or product designators as required.

3. Classification authority and declassification notation.

4. Preparing activity, agency and office symbol.

5. Do not use codewords on front or back covers. Use the special handling notation "APPENED DOCUMENTS CONTAIN CODEWORD MATERIAL".

b. Title page. If no cover page is used then the title page will include all information from paragraph 4.5.1 above. If the document has a cover page, mark the title page as follows:

1. Highest classification of the document spelled out and centered at the top and bottom.

a. SCI system caveat.

b. Dissemination control markings.

c. Special caveats or product designators.

c. First page. If the document has a cover or title page, mark the first page the same as an interior page. If the document does not have a cover or title page, mark the first page the same as a document cover.

d. Interior pages.

1. The highest classification of the material contained on that page and SCI code words, top and bottom. If a page does not contain classified material mark it as UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked at the top and bottom of each interior page when such marking is necessary to achieve production

efficiency and the particular information to which the classification is assigned is otherwise identified consistent with portion marking explained below.

2. Short form dissemination control markings at the top and bottom of the page following the classification.

e. SCI control system caveats at the bottom of all pages.

4-4. PORTION MARKINGS. Portion is defined as each title, header, or subject line; each part, such as illustration, photograph, figure, drawing, or chart; each paragraph and subparagraph; and similar portions.

a. Mark each portion according to its own classification and with other markings required by that portion. Use abbreviations for classifications (TS, S, C, U); SCI control system caveats; codeword's; product or project indicators; and ICD 710 control markings.

b. Mark titles with their proper classification. Unless the usefulness of the document would suffer, SCI document titles should be unclassified.

c. Placement of portion markings.

1. Place markings after the subject title, e.g. "Security (U)"

2. Place markings before the header. Headers do not have to be portion marked if they do not reveal any classified information. However, if one or more headers are classified, all headers must be marked.

3. Place the markings after the paragraph or subparagraph number or letter preceding the text.

4. Place markings within or contiguous to illustrations, photographs, drawings, or charts. Classify captions for these portions on the basis of their content and place markings immediately preceding the caption.

4-5. WORKING MATERIALS. Working materials are those materials created during the preparation of finished documents and material. Handle working material as follows:

a. Date when created and mark on the first page the notation "Working Papers-Destroy Within 90 Days".

b. Mark with the highest classification of any information contained therein; safeguard working materials according to the handling, storage, and disposition requirements for SCI documents. In the

II MEF SCIF all SCI material must be stored in GSA approved containers when not in use.

c. Destroy within 90 days of origin or place in SCI control channels.

4-6. SPECIALIZED MEDIA. The following are labeling requirements for specialized media.

a. Automated Information Systems (AIS) media. Each media item located in the SCIF will be marked with the highest classification processed. Marking of all media, with the exception of CD-ROM and DVD, will be accomplished using the appropriate standard form (SF-710, SF-711, etc.) to show its classification and SCI control system. AIS includes, but is not limited to, all CPU, printers, servers, removable or external hard drives, floppy disks, magnetic tapes, and copiers.

1. CD-ROM and DVD media will be marked using a permanent marker to write the classification and any caveats. The case will be marked utilizing the appropriate standard form.

2. Flash drives, thumb drives, memory sticks, and personal external hard drives are NOT authorized for use in the SCIF at any time.

b. Message Traffic. SCI transmitted by accredited electronic means, resulting in hardcopy, will be marked at the top and bottom of each page (including each segment of messages printed on perforated paper) with security classification and labeled to show all applicable SCI caveats, codewords, and product designators in accordance with DCID 6/6. The classification markings applied by printing equipment will be highlighted by spaces, asterisks, or slant bars. Portion marking applies to the message text. SCI message traffic will bear an appropriate classification block. SCI documents transmitted via facsimile are not message traffic and will be handled according to paragraph 7.

c. Graphic Arts material. Mark visual aids, map artworkS, blueprints, and such other material with the classification and SCI control system or codeword under the legend, title block, or scale, and at the top and bottom in such a manner as to be reproduced on all copies.

4-7. SCANNING CONTROL PROCEDURES. The SCI scanner and the SCIF must be approved and accredited for the appropriate classification and access level of the material processed. Individuals receiving the material will have the appropriate clearance, SCI access, and need-to-know.

a. All scanners will be approved and controlled by the SSO office and the ISSM.

4-8. SCI ACCOUNTABILITY. DoD policy is to eliminate accountability of SCI documents as a routine security protection measure. SCI material is non-accountable except material specifically designated as "accountable SCI" by the original classification authority. Designated accountable SCI will not be destroyed locally, instead, when no longer needed it will be turned into the SSO to be returned to the originator. The SSO will maintain an electronic record of external receipt and dispatch sufficient to investigate loss or compromise.

4-9. STORAGE. SCI material will be stored in a GSA approved safe when not in use. All safe combination changes will be completed by SSO personnel. This is to ensure the combination is recorded accurately and the change is done correctly. This will reduce the number of safes that must be opened by a locksmith.

4-10. REPRODUCTION. Reproduction of SCI documents will be kept to a minimum consistent with operation necessity. SCI will only be digitally reproduced in the SCIF.

a. SCI will not be reproduced on equipment used to reproduce unclassified or collateral information.

b. All prohibitions, to include reproduction, designated by the originator will be honored.

c. Copies are subject to the same control, accountability, and destruction procedures as the original document. Extracts of documents will be marked according to content and treated as working material.

4-11. DCS RECEIVED MATERIALS. All material shipped through DCS will be processed through the SSO office. When material is received from the Defense Courier Service (DCS), it will be logged by the SSO office and delivered to the appropriate office. The acknowledgement of receipt will be completed by the SSO and either mailed or faxed to the sender. DCS receipts and a copy of the acknowledgement of receipt will be maintained for 1 year in the DCS binder.

a. Damaged DCS Packages. If a package is received damaged from DCS, the SSO office will send an electronic message to the originator containing the following information.

1. Package number and organization from which received.

2. Specific material involved as well as an inventory of all material contained therein.

3. Possible cause and extent of damage. Include opinion concerning adequacy of packaging.

4. State if compromise of material occurred.

5. SSO must notify Commander/DCS, via immediate GENSER message, whenever DCS material is lost, damaged, compromised, destroyed, or mishandled. Include a statement giving the classification of the material and identifying the material as SCI. DO NOT identify the specific material.

4-12. DESTRUCTION. SCI material which is no longer required should be destroyed as soon as possible. Destruction must be in a manner to preclude reconstruction in an intelligible form. The majority of destruction accomplished will be by shredding. Accountable SCI will be turned in to the SSO by the appropriate custodian for return to the originator. Only NSA approved destruction devices will be used to accomplish destruction of SCI material.

a. NON-SHREDDABLE MATERIAL. Material which cannot be shredded such as acetate, Mylar, magnetic tape, hard drive platens, etc. will be given to the SSO for destruction. The SSO will DCS acetate and Mylar to NSA for destruction. Magnetic tape and hard drive platens will be degaussed locally by the II MEF G-2 ISSM.

1. The degausser must be certified annually. The contact information and procedure for certification are in the degausser folder located in the Administration file cabinet.

b. HANDLING OF BURN BAGS. Burn bags will be emptied and the contents shredded at the close of every workday. Burn bags will be marked with the highest classification of information to be placed in bag, owner of bag and date bag was placed into use. Permanent marker will be used to place marking on burn bags.

4-13. CONTROL OF GENSER LEVEL DOCUMENTS. All GENSER level documents will be controlled by the II MEF Classified Material Control Custodian (CMCC). If a GENSER document is received via DCS, it will be taken to the II MEF CMCC for assignment of a control number. Items picked up from the II MEF CMCC will be controlled prior to receipt. Any information classified Top Secret collateral must be stored in GSA approved containers when not in use. II MEF SSO does not have any authority over the II MEF GENSER security program.

CHAPTER 5
TRANSPORTATION OF SCI MATERIAL

5-1. DEFENSE COURIER SERVICE. The Defense Courier Service (DCS) provides a means to transport SCI materials from one command to another. All materials requiring DCS shipment will be brought to the SSO for approval and transmittal. The SSO will utilize the Defense Courier Advanced Transportation Control Movement Document (DC-ATCMD) website, https://trackerlite.wpafb.af.mil/DCATCMD , to schedule the shipment. This will be the primary means of transporting SCI material because it affords the greatest level of security. The II MEF G-2 account number is HKN 192/430154-NF06/II MEF SSO.

a. All outbound shipments will be double wrapped by the SSO in accordance with reference (d). In addition, an inventory of the package contents and an acknowledgement of receipt will be included with the material.

b. Over-night storage. From time-to-time DCS will have a requirement to store material in the SCIF over-night when conducting road missions. DCS will coordinate with the SSO Chief to ensure that adequate space is available for storage and that the SCIF is open and available for delivery and pick-up.

5-2. SENSITIVE COMPARTMENTED INFORMATION COURIERS. The transportation of SCI material outside of the physical confines of a SCIF poses a definite hazard to the security of the material. Personnel selected to transport SCI material will be mature, stable and capable of exercising good judgment and common sense in emergency situations. Couriers must exert every available effort within their means to safeguard the material entrusted to them while outside of a secure area. The SSO may appoint couriers for the transport of SCI material within the continental United States. SCI indoctrinated military personnel without regard to rank or grade may serve as couriers. Couriers will not be designated purely based on billet. Courier cards will only be issued to individuals that have a recurring requirement to transport SCI.

a. Appointment of Courier. Prior to being issued a courier letter (Appendix F) or card, each courier will receive a brief (Appendix F) on their responsibilities and procedures to be followed. They will also read appropriate extracts from the espionage law and execute a certificate acknowledging receipt of the courier card.

b. The individual will be issued the courier letter or card and familiarized with security requirements concerning custody and storage of materials. The courier will also be instructed on command procedures for handling courier cards. Courier cards will remain in SSO custody, filed in the individual's security folder, unless needed to transport material. Prior to use, the card must be logged out with the SSO. Log entry must indicate date of

receipt, card number, and person assigned. Courier will be required to review II MEF policy concerning the handling of courier card and handling of classified material in transit.

5-3. COURIER RESPONSIBILITY. It is the responsibility of every individual who is entrusted as a courier to follow the necessary guidelines to keep from compromising classified information.

a. Ground Transportation.

1. Courier will use a government vehicle when available. If a courier must use a POV or rental vehicle they will inform the SSO prior to departure.

2. One person may act as a courier. However, the SSO may require more than one courier if circumstances warrant. These could include the volume of material, mode of travel, travel through a high crime area, or sensitivity of the material.

3. If the material is to be transported more than 50 miles two couriers are required.

4. SCI will be maintained in the personal possession and under constant surveillance of the courier at all times. If an overnight stop is required the SCI material must be stored in a local SCIF.

5. SCI will not be read, studied, displayed, discussed, or used in any manner in a public conveyance or place.

6. SCI will not be hand-carried across international borders.

7. Round trip hand carrying of SCI will only be authorized under exceptional circumstances. DCS should be utilized to return the material.

8. SCI transported via vehicle must be stored within the vehicle. SCI will not be transported in any sort of external or removable luggage device. SCI material will not be left unattended.

9. SCI will be double wrapped prior to exiting the II MEF SCIF. SSO office must certify and approve the wrapping.

10. Couriers will not conduct any personal or other official business while acting as a courier.

11. Couriers will make no stops between point of origin and destination.

b. Air Travel. Transportation via commercial air requires additional steps in addition to those covered in ground transportation.

Commercial air carriers must be U.S. flagged. Transport via military aircraft does not required courier orders; however a courier card is still required to transport the material from the base to the aircraft. No foreign carrier may be used without the written approval of the II MEF Senior Intelligence Officer.

1. Couriers must be issued an original letter of authorization to use commercial air issued by the SSO, receive written special instructions, and will sign a statement acknowledging understanding of courier responsibilities (Appendix F).

2. Recurring or blanket courier letters of authorization for using commercial air will not be issued.

3. SCI must remain in the custody and physical control of the courier at all times.

4. Envelopes containing SCI are to be free of metal binders, clips, or other metallic objects that might "trigger" air terminal screening devices. If the envelopes are in a briefcase or carry-on-baggage, the briefcase or luggage may be opened for inspection. The screening officials may check envelopes by x-ray machine, flexing, feeling, and weighing. At no time will a screener open the envelope. If a screener insists on opening an envelope containing SCI material immediately ask to speak to a supervisor. There is a standing agreement between the Transportation Security Agency (TSA) and the intelligence community concerning the proper screening of couriers. The courier authorization letter must be presented to all screeners.

5. SCI material too large to be hand-carried will be shipped via DCS. In extraordinary situations when transportation via courier is the only available means a courier authorization may be requested from the AC/S G-2. If approved the following restrictions will also apply.

6. Although air carrier personnel will actually load and unload the SCI material, the courier will accompany the classified information and keep it under continual surveillance during loading and unloading. The courier must also be available to conduct visual observations at any intermediate stops if the cargo compartment is open. All arrangements must be made with the airline prior to departure. The courier must provide the SSO with a point of contact at the airline with which the arrangements have been made as well as the POCs to be contacted at origination, destination, and any intermediate stops.

c. All couriers will carry a phone roster of II MEF SSO personnel to contact in case of emergency. The roster will include both work and home numbers. Couriers are directed to contact the SSO for

additional direction or assistance if there is any situation which is out of the ordinary or the courier does not feel comfortable with. Couriers will also contact designated SSO personnel to report any deviation in travel plans.

5-4. COURIER CARD TURN IN/DESTRUCTION. The SSO will receive the card from the individual at the completion of their courier duty. If the card has not expired, it will be placed back into the individual's file for future use. If the card has expired, the card number will be removed from the card and placed in the courier card issue/destruction log. The date of destruction will be entered and the card will be destroyed in a NSA approved shredder.

a. LOSS OF COURIER CARD. Loss, theft or compromise of a courier card will be reported AS SOON AS POSSIBLE, to the II MEF SSO, regardless of the location of the loss, theft or compromise. Notification must include full circumstances surrounding the incident.

b. The SSO must report to SSO Navy all loss, theft or compromise of courier cards. The report will include all circumstances surrounding the incident to include actions taken to prevent further occurrence of similar incidents, and recommendations regarding issuance of a new card to the individual involved in the incident.

CHAPTER 6
SECURITY INCIDENTS

6-1. GENERAL. All actual or suspected incidents of compromise will be immediately reported to the SSO office. All actual or suspected incidents will be investigated immediately. In cases where a compromise has been ruled out and there is no effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level will be accomplished. The SSO Chief is the lowest appropriate level for resolving actual or suspected incidents. Regardless of resolution, all actual or suspected incidents of compromise must also be reported to SSO Navy via email immediately upon discovery. If it is determined no actual incident occurred, a follow-up email must be sent to SSO Navy to close out reporting.

6-2. SECURITY INFRACTIONS. A security infraction is defined as a failure to comply with provisions of security regulations which causes a potential compromise of classified information.

a. A security infraction requires immediate corrective action but does not require investigation. A security infraction is not a security violation, but could lead to a security violation if not immediately corrected.

b. All suspected security infractions will be reported to the SSO immediately. Examples of security infractions include, but are not limited to, courier carrying classified information stopping at a public establishment, placing burn bags adjacent to an unclassified trash container, failing to wear identification badge correctly, or failing to change security container combinations as required.

c. Individuals responsible for a security infraction will be issued a written letter by the SSO which identifies the security infraction and provides corrective action (Appendix H).

d. Personnel that commit two or more security infractions in a six month period will have their SCI access suspended and a Subject Access Eligibility Report (SAER) (Appendix O) will be submitted to DODCAF to re-evaluate the individual's continued eligibility for SCI access.

6-3. SECURITY VIOLATION. A security violation is defined as a compromise of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of security regulations which is likely to result in compromise.

a. All security violations require investigation. Violations can result from, but are not limited to, deliberate or accidental exposure of SCI resulting from loss, theft, or capture; recovery by salvage; defection; press leaks or public declarations; release of

unauthorized publications; or other unauthorized means. The two most likely events to occur within the II MEF organization are deliberate or accidental exposure to unauthorized persons, and loss during tactical operations or exercise. All SCI indoctrinated personnel must be especially diligent when un-cleared persons are working within the SCIF and when conducting operations in a Tactical or Mobile SCIF.

b. Loss or exposure of SCI from any cause requires immediate reporting, investigation and submission of a damage assessment describing the impact to national security.

c. Compromise as a result of espionage or suspected espionage will be reported immediately to SSO NAVY if detected by SSO personnel. All activity concerning the violation will cease pending a counterintelligence assessment by SSO Navy or a designee. Other personnel who suspect espionage will contact the Federal Bureau of Investigation or NCIS immediately. Personnel will not inform the SSO or any other command member. Personnel will not attempt to investigate or stop the activity.

d. Other incidents where a certain compromise will immediately be reported to the Community Program Manager (The CPM will vary depending caveat of the information) via SSO Navy. The Director, National Intelligence must be provided summaries of investigations, via SSO Navy and Intelligence Community Program Manager, if the investigation reveals SCI was inadvertently disclosed to foreign national(s), or deliberately disclosed to unauthorized persons. This reporting requirement also exists if the investigation involves espionage, flagrant dereliction of security duties, or serious inadequacy of security policies and procedures.

e. All serious security violations occurring on a computer system, terminal, or equipment which processes SCI will be reported to SSO Navy with information copies to SSO DIA/DAC-3D/SYS-4. Computer security incidents will be reported according to ICD 503. SSO and ISSM will coordinate investigating security incidents involving computers. Examples of serious computer security incidents include, but are not limited to:

1. Human error in reviewing media for content and classification, resulting in compromise.

2. Incorrect settings of a security filter that result in compromise.

3. Intrusion attempts, either physical or through the IDS/computer system.

4. Virus attacks.

5. Failure of a system or network security feature.

f. SCI security violations that could impact an individual's continued eligibility for access to SCI will be reported to DODCAF.

6-4. SECURITY INQUIRY. All security violations must be reported to SSO Navy, information copy to SSO DIA/DAC-3D, and the local SIO immediately upon discovery. Interim reports must be submitted to the local SIO, information copy SSO DIA/DAC-3D every 30 days until the final report is submitted. All inquiries and investigations will be conducted in accordance with reference (d).

a. Security Inquiry. The local SIO must appoint an inquiry official. The inquiry official will submit a written Report of Inquiry to the local SIO via the SSO. The SIO must refer the incident for formal investigation if the Report of Inquiry finds there is a reasonable likelihood of compromise.

b. Conduct of Investigation. The investigation will determine if there is a reasonable likelihood that a compromise of SCI may have occurred, the identity of the person(s) responsible for the unauthorized disclosure, and need for remedial measures to preclude a recurrence. The investigation should reveal the following from the time the violation started to the time it was discovered and corrected.

c. Corrective Action. Investigation officials will advise SSO Navy of weaknesses in security programs and recommend corrective action. SSO Navy is responsible for ensuring appropriate corrective action is taken in all cases of actual security violations and compromises.

1. Administrative sanctions imposed in cases of demonstrated culpability will be recorded in security files.

2. Except in instances where immediate action is necessary, an individual found responsible for a security incident will be afforded the opportunity to present information in their defense prior to implementation of administrative sanctions. Remedial sanctions may be applied by SSO Navy according to the severity of the incident.

d. Damage Assessments. The assessment considers how the loss or compromise of material could result in damage to the national security or place the U.S. at a disadvantage. Format for damage assessment is appendix I. Damage assessments are used to:

1. Reevaluate lost or compromised information.
2. Determine if changes in classification are appropriate.
3. Indicate damage to the national security.

e. Case File Retention. Case files will be retained locally for a minimum of 2 years or until no longer needed. Case files referred

to the Department of Justice or Department of Defense for prospective determinations will be retained for 5 years after the closure of the case. The files will be destroyed locally when no longer needed.

f. Inadvertent Disclosure Agreements. The SSO will exercise their best judgment as to whether the interests of SCI are served by seeking written agreements from non-indoctrinated persons to whom SCI was inadvertently disclosed. If the person signs an inadvertent disclosure agreement and the SSO has reason to believe that the person will maintain absolute secrecy concerning the SCI involved, the report of investigation may conclude that no compromise occurred. Copies of executed inadvertent disclosure agreements will be maintained as part of the Report of Investigation.

6-5. REPORTING MISSING PERSONNEL. All personnel who have current SCI access or past access to SCI who are killed, captured or missing in action, absent without leave or similar circumstances must be reported to SSO Navy by priority message within 72 hours of discovery. The following will be reported.

a. Name
b. Rank
c. Social Security Number
d. Organization
e. Summary of information that may be compromised

1. Individuals, who are killed, except SCI couriers or those participating in unauthorized hazardous activities, need not be reported when it is known that death was instantaneous and no possible interrogation could have occurred.

6-6. REPORT OF SCI APPEARING IN THE PUBLIC MEDIA. All personnel must be cognizant that the publishing of SCI in the public media does not constitute declassification, decompartmentation, or relaxation of SCI security policy. SCI-indoctrinated personnel should not comment on, confirm, or deny information from open source articles or discussion of an SCI nature. Acknowledging information of an unauthorized nature can add to the damage or lend credibility to the unauthorized disclosure. Do not mark the article or indicate in any way that it contains SCI. Do not discuss the article outside the SCIF.

a. Any SCI-indoctrinated individual that recognizes SCI matter in public media will immediately notify the SSO through secure means.

b. SSO will report the incident to the local SIO, SSO Navy and SSO DIA/DAC-2B.

1. The report will be classified according to content, minimum of CONFIDENTIAL to prevent further disclosure. It will be sent via

priority record message or secure facsimile and will provide the following information:

a. Type of media, date of medium, title/headline, and name of author.

b. Classified intelligence disclosed. Either quote the information or provide a synopsis. DO NOT transmit the actual article via facsimile unless requested.

c. Identify the classification source of the material.

d. Initial damage assessment.

CHAPTER 7
AUTOMATED INFORMATION SYSTEM SECURITY

7-1. GENERAL. Reference (g) delineates procedures for Automated Information System (AIS) security in general. The following paragraph specifies requirements for AIS security at the II MEF Sensitive Compartmented Information Facility (SCIF). Specific information concerning AIS security can be located in the SCIF Automated Information System (AIS) Security Plan and current directives.

7-2. PHYSICAL SECURITY OF II MEF AIS SYSTEMS. All AIS's processing SCI within II MEF will be physically located within the SCIF. In addition, SCI will not be processed on any AIS within the II MEF SCIF unless those AIS have been approved for the handling of SCI information. These systems will be appropriately marked. Approval is made for the complete system and the system unit integrity must be maintained. Operating an SCI AIS outside of the II MEF SCIF is specifically prohibited unless specific written permission is granted by higher authority. Such requests will be handled on a case-by-case basis, in accordance with current directives.

7-3. Joint Worldwide Intelligence Communications System (JWICS) was created in the early 90's during Operation Desert Shield/Desert Storm to allow the military to access SCI information from the intelligence community. JWICS is the intelligence community's proven global backbone network and provides its Department of Defense (DoD) and intelligence community customers with a mature, reliable, and flexible SCI architecture. Its mission is the delivery of secure, assured, efficient, interoperable information services on a global basis to national and defense intelligence consumers around the world.

a. ACCOUNT ACTIVATION. JWICS access is given on an as needed basis to individuals who have a recurring need to utilize the SCI network and are adjudicated to SCI eligibility via DODCAF. Interim SCI access is not allowed to a JWICS account. Simply having access to SCI does not mean that an individual has a requirement to have a JWICS account. Personnel requiring an account will receive the necessary paperwork from the II MEF G-2 RNOC. The individual will turn in the completed paperwork to the II MEF RNOC. Prior to being issued a user name and password the individual must complete the Cyber Intelligence Course via MarineNet. (Course Code: CYBERINTEL)

b. POLICIES TO MAINTAIN AN ACCOUNT. JWICS access is granted under the condition that individuals follow all policies and procedures governing its use.

1. These policies include but are not limited to account holders not allowing other individuals, including individuals with SCI access, to use their account.

2. Access information for which the user has a clear need-to-know.

3. Using only appropriately marked writable media to electronically copy information.

4. Completing annual system training.

5. Violating any of these policies can result in a revocation of the individuals JWICS account and SCI eligibility.

CHAPTER 8
CABLE TELEVISION

8-1. GENERAL. II MEF has been authorized to have a "mission essential" cable television system within the SCIF. This system will only be used to monitor, compare and verify fast breaking events as reported by television news media with those reports provided by the intelligence community. Additionally, this system is to be used to enhance intelligence information being provided to Crisis Action Cells when formed in the event of contingency operations.

8-2. SECURITY REQUIREMENTS. During operation, a three (3) foot physical separation must be maintained between the television set(s) and all classified computer systems. When not in use, the television set(s) are to be unplugged from the power source and the coaxial cable physically disconnected to prevent any possible penetration of the system. TV/VCR combos will not be used to view classified videos while coaxial cable is connected to the TV. Any questions concerning the proper use of televisions within the SCIF will be addressed to the SSO.

CHAPTER 9
SSO ADMINISTRATIVE FUNCTIONS AND GUIDELINES

9-1. GENERAL. The administrative functions of the SSO are its primary mission. Adjacent and/or subordinate units that conduct daily operations in the SCIF are required to support SCIF functions; to include SSR duties for II MEF. Some of these duties will require a temporary assignment of duty to the MEF. These assignments will be at the discretion of the SSO. Standard day-to-day operations consist of; processing T5/R (Formally known as SSBI/PR), handling Subject Access Eligibility Reports (SAER), Letters of Intent (LOI), Letters of Notification (LON), and determinations from DODCAF, as well as processing clearance certifications, transfers, debriefs, T5 and lateral-move interviews, foreign travel briefings, courier control and education, maintenance of SCI SMO in JPAS, and indoctrinating personnel. This chapter provides a brief overview of the policies and procedures for the administrative function of the SSO.

9-2. IDENTIFICATION OF SCI BILLETS. All SCI billets within the II MEF organization are identified on each unit's T/O. All additional SCI billets must be approved in writing (Appendix K) by the II MEF SIO. Commanding Officers will need to submit Table of Organization & Equipment Change Request (TOECR) to HQMC in order to change billet clearance requirements; once this is complete, Commanding Officers may submit Billet Nomination requests for SCI billets via the SSO. The request must include an unclassified justification that clearly establishes need-to-know to accomplish the unit's mission.

a. Billets with a need-to-know will be compared to the Billet Identification Codes (BIC) provided by the II MEF G-1 in accordance with reference (m).

b. All Billet Nomination Requests, approved or denied, will remain on file in the administration file cabinet.

9-3. PRE-SCREEN INTERVIEWS. Pre-screening interviews (Appendix L) are conducted to determine the initial eligibility to continue processing for SCI eligibility determination by DODCAF. This interview does not determine the final outcome of their access determination. This interview is simply a tool to allow the SSO to determine: additional information or material needed to process their investigation, likelihood of eligibility being granted, and to allow Headquarters Marine Corps to authorize or deny lateral-move requests. The ultimate goal of the pre-screening interview is to determine if the individual meets the basic requirements in reference (f) to be processed for SCI. This interview is conducted for individuals who have never had access to SCI, for Interim Clearance Requests and Lateral moves into MOS's requiring SCI eligibility. The completed questionnaire is protected under the Privacy Act of 1974 and is only viewed by the SSO personnel. It cannot be forwarded to the individual's chain of command.

a. Upon completion of the Lateral Move Interview, a SSO letter is typed and provided to the individual with a recommendation concerning continued processing. The interview and file copy of the SSO letter (appendix M) will be stored in the SSO office for one year in the Personnel file cabinet and then destroyed.

9-4. ELECTRONIC QUESTIONNAIRES FOR INVESTIGATION PROCESSING (E-QIP). E-QIP is the primary method of submitting T5/R throughout the DoD, and will be utilized by all II MEF personnel. E-QIP is part of the e-government initiative, sponsored by the Office of Personnel Management (OPM). E-QIP allows applicants to electronically complete the SF-86 forms, and transmit their completed data to our SSO office for review. The SSO personnel will review the electronic forms for completeness, and then forward them directly to OPM. E-QIP has the potential to greatly decrease turnaround time on investigations. E-QIP is accessible on www.opm.gov/e-qip. Specific directions on the use of E-QIP are located in the E-QIP handbook.

a. Tier 5 (T5). T5's are submitted for an individual's initial eligibility determination for SCI or collateral TOP SECRET. A pre-screening interview will be conducted prior to initiating a T5. This investigation covers a scope of the last 10 years or to the age of 16, whichever is less. The questionnaire covers all aspects of the individuals history to include residence, employment, finances, drug and alcohol use, criminal activity, foreign activity, family members and history, and previous security investigations (to include previous security clearances at lower levels, i.e. Secret). This questionnaire is filled out by the individual and then verified by the SSO prior to submission to the Office of Personnel Management (OPM) for investigation. In addition to the security questionnaire, the individual will schedule with the SSO to submit their fingerprints digitally.

b. Tier 5 Review (T5R) SUBMISSION. T5R's are submitted every 6 years to maintain SCI eligibility. The submission of the T5R is required 6 years from the investigation completion date reported by OPM of their last T5, T5R, SSBI or SBPR. Do not confuse the investigation date with the adjudication date. The questionnaire covers a scope of the last 7 years. If the individual has not submitted a T5R in 7 years, a new T5 must be submitted and the individual must be debriefed from SCI accesses. A T5R interview (appendix L) is conducted prior to the initiation of the individuals E-QIP.

c. Continuous Evaluations. The process can be used in lieu of T5R if there is no signification derogatory changes in subject's background information.

9-5. PROBLEMS WITH INVESTIGATION COMPLETION. Many problems can arise during the course of a security investigation. These problems often delay OPM's completion of the investigation and DODCAF's final adjudication. These can include but are not limited to, excessive derogatory information, information that was not disclosed in the security questionnaire, incorrect information in security questionnaire, and deployment.

a. An increasing problem is the subject not being available for the personal interview due to deployment. The SSO office must maintain a continual awareness of those indoctrinated, or eligible, personnel who are approaching the end of their previous investigation scope. THE ONLY WAY TO MITIGATE THIS PROBLEM IS TO BE PROACTIVE. OPM has initiated the "Catch them in CONUS" program to support the investigative process of deploying personnel. The SSO must contact OPM to have an individual assigned to the program.

b. REQUEST TO RE-OPEN INVESTIGATION. In the event that an individual is deployed while their clearance investigation is being conducted, their investigation may close short of scope due to a lack of subject interview. The investigation will remain closed until a subject interview can be conducted. When this occurs, a request to re-open is sent by the SSO to OPM. Prior to requesting the investigation be re-opened, the SSO will verify by personal contact that the subject will be available for at least 3 months. If the individual is going to be re-deploying within 3 months the SSO will contact OPM to have the individual assigned to the "catch them in CONUS" program.

c. REQUEST TO EXPEDITE. In the event that an individual will need access to SCI to complete mission essential tasks, i.e. Formal training prior to deployment, a request to expedite an interim determination may be submitted to OPM/DODCAF. Requests to expedite will not be submitted based purely on convenience. The meaning of expedite will vary depending on the agency.

1. OPM. If the request to expedite is submitted to OPM it will result in the National Agency Check with credit (NACLC) being completed sooner. This is not a determination of eligibility, it is only a tool used by DODCAF to determine eligibility.

2. DODCAF. DODCAF may grant interim access to SCI if a current NACLC has been completed and NO derogatory information was found during prescreening. Request will be made utilizing DISS.

9-6. FINAL ADJUDICATION OF CLEARANCE ELIGIBILITY FROM DEPARTMENT OF DEFENSE CENTRAL ADJUDICATION FACILITY (DODCAF). DODCAF is the authority for all security clearances eligibility determinations for Navy and Marine Corps personnel. After an individual's investigation is completed by OPM, it is sent to DODCAF for adjudication. When an individual is adjudicated they are granted eligibility to a specific level of classified material, i.e. SECRET, TOP SECRET, SCI. It is important to note that an individual may be granted access to TOP SECRET information without being granted access to SCI. This eligibility is what allows an individual to be granted access to SCI if they possess the necessary need to know associated with the security access. An individual granted access to SCI may be indoctrinated for any compartment. However, the indoctrination of individuals must be limited using the need-to-know concept. An individual will never be indoctrinated into any compartment based solely on rank or convenience.

a. NEED-TO-KNOW. The first personnel security principle in safeguarding SCI is to ensure only those persons with a clearly identified need-to-know are granted access to SCI. Need-to-know is a determination, by an authorized holder of classified information, that access to that information is required by another person to perform official duties. Individuals who possess classified information have the authority to give other individuals, who are appropriately cleared, classified information, or to deny them access to it. No person will be deemed to have need-to-know solely by virtue of rank, title, or position.

b. REQUEST FOR INTERIM ACCESS. In the event that an individual requires access to SCI before their investigation is complete, a request for interim access is requested. This is done when the investigation has been started, the subject has no foreign born spouse, family members or relationships, and there is no significant derogatory information found during a NACLC. Interim access allows indoctrination into SCI access programs based on DODCAF's belief that final adjudication will be granted upon completion of the investigation. Interim access requests should be treated as the exception, not the rule. If it is not absolutely essential to the accomplishment of the mission individuals will not be indoctrinated until final adjudication is granted. Commanding Officers may identify this requirement, in writing, to the SSO.

1. Basic requirements for interim access are a favorably completed NACLC, favorable security interview, and an open T5.

2. When indoctrinated under interim access, individuals should have access to the minimum SCI material required to perform their required duties.

9-7. DEROGATORY INFORMATION REGARDING SCI ELIGIBLE PERSONNEL. Derogatory information may be reported and may delay the investigation and/or result in an unfavorable eligibility determination. There is a standard process in place to support the reporting of such information, dissemination of DODCAF decision, and the individual's right to appeal any unfavorable decision.

a. SECURITY ACCESS ELIGIBILITY REPORT (SAER). SSOs and supervisors at all levels are responsible for being aware of and reporting immediately any information which might affect an individual's continued ICD 704 eligibility for SCI access. The SAER format is provided in Appendix O.

1. Report to DODCAF, info SSO NAVY and HQMC, all pertinent facts to determine an individual's eligibility for continued access. Incidents involving the person's immediate family should be reported when ICD 704 eligibility is or might be affected.

2. Forward a SAER when:

a. Directed by DODCAF, SSO Navy

b. An individual is debriefed for cause.

c. Access has been suspended for more than 90 days.

d. Any information reflecting adversely on a persons' eligibility for access to SCI becomes known.

e. A persons association with foreign nationals exceeds what would be considered normal for the circumstances, or may pose a potential security risk.

f. Criminal activity, to include sexual offenses and deviant sexual behavior.

g. The loss, compromise, or unauthorized disclosure of classified information, or a recurrence of practices dangerous to security.

h. Alcohol abuse or misuse, including multiple arrests for alcohol-related incidents.

i. Radical or unexplained changes in behavior and/or serious family problems.

j. Serious mental or emotional problems.

k. Serious financial problems, including filing for bankruptcy or wage earners plan (a personal financial statement (Appendix P) must be forwarded with the SAER).

l. Individual does not screen for overseas duty.

m. Any of the questions in Part 1 of the SAER that can be answered yes.

n. The CO/OIC/SSO deems it appropriate.

3. The SAER must include a specific command recommendation whether the subject of the report should have continued access and under what conditions, or should the individual be issued a Letter of Intent (LOI) or Letter of Notification (LON). If the recommendation is for ineligibility, the CO/OIC must personally sign the SAER. This requirement is to inform the DODCAF that the CO/OIC is fully aware of the contents of the SAER and the recommended action.

4. If a person transfers to another command with an SSO during a period of observation, or conditional security determination, the losing SSO will forward copies of all pertinent documents to the gaining SSO, with a copy of the transmittal letter to DODCAF, info copy SSO Navy.

5. A decision to either continue the person's access to SCI or be debriefed for cause may be directed by SSO Navy. If the person is to be transferred from the local area for treatment, and access has not been otherwise been suspended, the person shall be debriefed for cause.

6. All SAERs will include a II MEF SSO endorsement.

b. Conditional Security Determination. DODCAF may issue a conditional security determination, or probation, when the information or investigation has been reviewed, and a favorable determination has been made that the individual meets ICD 704 standards even though derogatory information contained in the investigation or the report is significant, and a serious concern. The individual will be cautioned that further receipt of derogatory information or their failure to comply fully with the identified condition(s) is cause for immediate reconsideration of access. The command may be advised that monitoring and observing the individual is required, and may be required to submit periodic observation report to the DODCAF.

c. Letter of Intent (LOI). The DODCAF issues a LOI to the individual, via the SSO advising him/her of the intention to deny or revoke SCI eligibility. When a LOI is issued, the SSO will immediately request a 45 day extension, the command will follow the procedures contained within the LOI, and the subject will be made aware of his/her right to provide material on their own behalf. A CO's recommendation or endorsement is required and will, along with any additional information, favorable or unfavorable, be given full

consideration. The SSO Chief is responsible for the handling of all LOIs.

1. The SSO, with the advisement of the CO/OIC, and based on the mission and operational commitments, determines whether the individual will be immediately removed from access or remain indoctrinated pending a final DODCAF decision. If a decision is made to retain the individual in SCI access, immediately notify SSO Navy of the reasons for the decision.

d. Letter of Notification (LON). A LON may be issued by DONCAF after consideration of the individual's written response to the LOI, upon notification by the individual that they do not intend to respond, or lacking a response within the required suspense date. If the individual's security clearance and eligibility are denied or revoked, the LON will state the reasons for the determination, and inform the individual of their right to appeal the decision in writing directly to the Personal Security Appeals Board (PSAB) or personally present a verbal appeal via a Administration Judge of the Defense Office of Hearing and Appeals (DOHA), which will be transcribed and provided ultimately to the PSAB. The SSO Chief is responsible for the handling of all LONs and assisting in the preparation of correspondence with the appropriate appeals office.

9-8. CLEARANCE CERTIFICATION. Clearances are verified at each individual SSO for the personnel that work in that area. When personnel visit other facilities outside II MEF control a clearance certification is passed to verify an individual's clearance and accesses.

a. Clearance Certification will be passed as follows:

1. For commands and organizations within the Department of Defense, clearance will be delivered via JPAS.

2. For commands and organizations outside the Department of Defense, clearance will be passed via record message traffic.

b. Clearance certification falls into two categories.

1. Visit certification. A visit cert is a clearance certification for a specific organization, for a specific purpose, for a specific time period. I.E. formal school, conference, meeting, etc.

2. Permanent Certification is a clearance certification for a specific organization which an SCI indoctrinated individual has a recurring need to visit for official purpose. A permanent certification can be approved for up to 12 months.

a. If an individual is debriefed for any reason or transferred to another command or organization any permanent certification must be formally cancelled.

9-9. TRANSFER IN STATUS. A transfer in status (TIS) must be requested by a member's gaining command, and can only be completed for SI and TK accesses. There are no other accesses authorized for TIS. Any access outside of SI and TK must be debriefed prior to a member's departure with a TIS in effect. The individual will be dropped from all II MEF access rosters and their badge disabled if not already done. If an individual fails to check out with the II MEF SSO, and no request for ownership is received within 30 days, they will be administratively debriefed from all SCI accesses and their file will be slated for destruction. This is to ensure that individuals retain no accesses to Sensitive Compartmented Information that they no longer have a need-to-know.

a. For locations not under the control of the Marine Corps, Navy or DIA, a transfer in status message will be sent, if requested by the gaining unit/organization. The individual will be debriefed from any compartments not identified as required by the gaining command/organization. The SSO office will respond by record message traffic using format in Appendix Q.

b. Transfer to a contractor. The SSO office may transfer the ICD 704 eligibility of military personnel to a contractor organization if:

1. The individual has been selected for employment with the respective contractor.

2. The duties to be assigned have been approved with a need-to-know and are assigned to a current SCI contract.

3. Defense Industrial Security Clearance Office (DISCO) has been notified of the transfer of ICD 704 eligibility.

4. The message request from the contractor must include verification of the above as well as the name and expiration date of the contract.

9-10. INDOCTRINATION. Indoctrinations are the instructions an individual receives prior to receiving access to an SCI system or program. These instructions convey the unique nature, unusual sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods. The SCI indoctrination process will include:

a. The update of information listed on the individual's E-QIP. Our office will insure that any information not previously reported, or any incident(s) that have occurred since the previous Personnel Security Questionnaire was completed is included.

b. The signing of a Non-disclosure Agreement (NdA).

c. A briefing on the authorized SCI access (es). All indoctrinations will include the appropriate indoctrination video(s).

d. Recite verbal attestation.

e. A brief on outside activities will be made available to everyone who is indoctrinated for SCI access.

f. A brief on local policies.

g. INDOCTRINATION ASSIST. In the event that an SCI eligible individual requires access to SCI but is unable to be indoctrinated by their owning SSO, indoctrination assist is requested. This involves the same procedures as indoctrination, however the paperwork is sent to the owning SSO upon completion of the indoctrination.

h. FOREIGN FAMILY MEMBERS. In the event that an SCI eligible individual requires access to SCI but has documented, foreign citizen family members, a risk acceptance letter must be completed and signed by the SIO prior to indoctrination.

9-11. DEBRIEF. When the need-to-know for SCI has ceased or an individual's access to SCI is terminated for cause, the individual will be denied further access to SCI. Upon retirement or separation all collateral clearances and SCI access immediately terminate. The SSO is responsible for accomplishing and reporting the debrief action and for cancelling all current visitor certifications pertaining to the debriefed individual. Debriefings will include:

a. Individual reads appropriate sections of Title 18 and 50 of the United States Code.

b. Acknowledgement of the continuing obligation of the individual under prepublication review and other provisions of the NdA never to divulge, publish, or reveal by writing, spoken word, conduct or otherwise, to any unauthorized persons, any SCI without the written consent of appropriate department/agency officials.

c. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation, or the department/agency, any attempt by unauthorized person to solicit national security information.

d. A reminder of the risks associated with foreign travel.

e. The signing of a DD Form 1848. The DD Form 1848 is unclassified when using the DCI approved digraph or trigraph.

9-12. FOREIGN BORN EXCEPTION PACKAGE. In the event that an individual who has access to SCI intends to marry a foreign individual or an individual who is requesting access to SCI has foreign family members, a foreign born exception package has to be submitted on the individual. An individual with foreign born immediate family member(s) is not eligible for access to SCI per reference (f) Annex C. An exception can be requested if the individual has a skill that is essential to the continued success of the Marine Corps. This would be considered a "Compelling Need". The skills possessed by the individual must be needed to prevent failure or serious impairment of missions or operations that are in the best interest of the national security. If the Commanding Officer feels that the risk is acceptable he/she will submit a request for compelling need exception (Appendix Z). Every country has been designated a Tier based on the threat level of that country. Based on the Tier level of the country their family/spouse is a citizen of, the following will also be completed by the applicant:

a. Provide SSO of intent to marry 120 days prior to marriage.

b. Counterintelligence (CI) interview. (Tier II)

1. After CMC SSO has endorsed the exception - CMC will schedule a Counterintelligence Scope Polygraph with NCIS.

c. Compelling Need statement.

d. Intelligence Risk Assessment.

e. Subject Acknowledgement Statement

f. Subject Acknowledgement Memorandum, in accordance with BANIF 20-03

g. Requirements to Adjudicate Memorandum

h. Foreign Born Spouse Statement of Person History (if applicable).

i. Foreign Contact Interview; one for each contact and/or in-law etc. (not required for spouse)

j. NATURALIZED Spouse or other naturalized immediate family member; provide the following items:

1. Provide "Proof of Naturalization" and "Proof of citizenship" for all countries where citizenship was held and the former "Country of birth verification" translated into English.

2. Additionally include a signed individual statement stating whether they do or do not hold a foreign passport and do or do not claim dual citizenship status with their former country of citizenship.

k. NATURALIZED Spouse or other naturalized Immediate Family member claiming dual citizenship status:

1. Provide "Proof of Naturalization" and "Proof of citizenship" for all countries where citizenship was held and the former "Country of birth verification" translated into English.

1. Provide a signed memorandum addressing:

1. Detailed circumstances under which the individual met his/her spouse/prospective spouse.

2. Inclusive periods of association and nature of their association prior to the decision to marry.

3. Date and place of projected marriage.

4. Listing of relatives of the spouse/prospective spouse who have been met and the frequency and nature of contact with them.

5. Statement of member's feelings of affection or obligation to members of his/her spouse's/prospective spouse's immediate family.

6. If foreign national is in the U.S., when he/she arrived (date and point of entry).

7. How often does the spouse/prospective spouse visit his/her native country and for what reason.

8. If the spouse/prospective spouse and/or any members of his/her immediate family are involved in political activities in their native country, describe their activity and political affiliation. Include a statement if they are not politically involved.

9. Whether spouse/prospective spouse or any of his/her relatives have shown any interest in or have questioned member regarding his/her duties or any classified information he/she may have access to.

10. Acknowledgement that marriage to a foreign national may adversely affect member's current assignment and/or SCI eligibility.

11. Provide the following documents from spouse/prospective spouse. All documents must be in English.

a. SF86 - Personnel Security Questionnaire, omitting blocks 20, 21, 22 and 24 through 28.

b. Copy of birth certificate, or other evidence of current citizenship. If the documentation is in a language other than English a certified translation must be submitted along with a copy of the original.

m. SCI indoctrinated individual's cohabitating or involved in a continuing intimate relationship with a foreign national shall:

1. Notify SSO within two weeks of initiating the close association/cohabitation.

2. Provide up-to-date personnel security questionnaire.

3. Provide a signed memorandum addressing the following:

a. Detailed circumstances under which the member met the foreign national.

b. Inclusive period of association.

c. Frequency of contact and conditions under which contact has been accomplished.

d. Nature and extent of any feelings or affection or obligation to the individual.

e. Whether the foreign national has ever shown interest in or requested information regarding his/her duties or any classified information he/she may have access to.

f. Obtain from the foreign national all information as required for spouse/prospective spouse with the exception of statement of intent towards U.S. citizenship.