

This is the html version of the file

[http://www.usmc.mil/directiv.nsf/0/788f70925ede0bf28525680f005e25a0/\\$FILE/MCO%205511.18A.pdf](http://www.usmc.mil/directiv.nsf/0/788f70925ede0bf28525680f005e25a0/$FILE/MCO%205511.18A.pdf)

Google automatically generates html versions of documents as we crawl the web.

To link to or bookmark this page, use the following url: <http://www.google.com/search?q=cache:qg6gx37oQPAJ:www.usmc.mil/directiv.nsf/0/788f70925ede0bf28525680f005e25a0/%24FILE/MCO%25205511.18A.pdf+%22CJCSI+3231.01%22&hl=en>

q=cache:qg6gx37oQPAJ:www.usmc.mil/directiv.nsf/0/788f70925ede0bf28525680f005e25a0/%24FILE/MCO%25205511.18A.pdf+%22CJCSI+3231.01%22&hl=en

Google is not affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: **cjcsi 3231.01**

Page 1

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

MCO5511.18A

PLN-8

30 Oct 98

MARINE CORPS ORDER 5511.18A

From: Commandant of the Marine Corps

To: Distribution List

Subj: POLICY FOR SAFEGUARDING THE SINGLE INTEGRATED OPERATIONAL PLAN (SIOP)

Ref: (a) CJCSI 3231.01 (NOTAL)

(b) OPNAVINST S5511.35K

(c) OPNAVINST 5510.1H

(d) MCO P5510.18

Encl: (1) Procedures for Safeguarding the Single Integrated Operational Plan
Within Headquarters Marine Corps

1. Purpose. To implement within Headquarters Marine Corps (HQMC), the Joint Chiefs of Staff (JCS) policy for safeguarding the Single Integrated Operational Plan (SIOP).

2. Cancellation. MCO 5511.18

3. Information

a. Reference (a) provides JCS guidance for safeguarding SIOP and SIOP-Extremely Sensitive Information (ESI).

b. Reference (b) implements the JCS policy and contains instructions for safeguarding SIOP and SIOP-ESI for all Navy and Marine Corps commands and activities. Included in reference (b) are detailed instructions concerning definition, identification, classification, distribution, inventory, access category, briefing, correspondence, data processing, and destruction of SIOP and SIOP-ESI materials. Reference (b) also sets forth travel

restrictions
on personnel possessing broad and substantial knowledge of programs considered
to be vital to the security of the United States.

c. References (c) and (d) provide information for the safeguarding of
classified information in the Department of the Navy and HQMC, respectively.

4. Action. All personnel at HQMC who have access to or receive SIOP
materials
will safeguard such materials per references (a) and (b) and the enclosure of
this Order.

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

Page 2

MCO 5511.18A
30 Oct 98

5. Summary of Revision. This Order has been updated throughout. It should
be
read in its entirety to ensure a complete understanding of the policies and
procedures contained within.

DISTRIBUTION: PCN 10208540200

Copy to: 7000110 (55)
8145005 (2)
7000099,144/8145001

2

MCO 5511.18A
30 Oct 98

PROCEDURES FOR SAFEGUARDING THE SINGLE INTEGRATED
OPERATIONAL PLAN WITHIN HEADQUARTERS MARINE CORPS

1. Responsibility. In accordance with references (a) through (c), and as directed by reference (d), the Deputy Chief of Staff for Plans, Policies and Operations (DC/S PP&O)(PL) is responsible for the administration of the SIOP-Extremely Sensitive Information (ESI) Special Access Program.

2. Access and Access Control

a. General Requirements. General requirements for controlling access to SIOP materials are contained in reference (b).

b. Limiting Access. Access to SIOP-ESI materials will be on a selective and discriminating basis and will be limited to those categories of information which are essential to carrying out the duties assigned to an individual. Categories of operational and administrative access to SIOP-ESI

are described in reference (a).

(1) Establishment of Specific SIOP-ESI Billets. Heads of staff agencies shall identify specific billets which require access to SIOP-ESI information on a continuing basis. A listing of such billets, to include the billet title, Service, SIOP access categories granted, SSN and full name will be maintained by DC/S PP&O (PL).

(2) Temporary SIOP-ESI Access. Requests for temporary SIOP-ESI access for personnel not occupying billets requiring permanent SIOP-ESI access will be held to an absolute minimum. The request will include an appropriate termination date. Authorization for access based on possible future need will not be granted. Visits to commands or participation in activities which require temporary access to SIOP-ESI will be coordinated with DC/S PP&O (PL).

c. Requests for Access to SIOP-ESI. Consistent with the requirements for limiting access described above, the following procedures will be used to obtain SIOP-ESI access for HQMC personnel:

(1) Heads of Staff Agencies will:

(a) Request to PP&O (PL) via e-mail, telephone conversation or letter that an individual be given access to SIOP-ESI. Request should include name, rank, SSN, office code, date and place of birth of the person for which access is being requested.

(b) Ensure that the individual, upon transfer, detachment, or when the individual no longer requires access, reports to the DC/S PP&O (PL) for debriefing and termination of access.

(2) The DirAR (ARFD) will:

(a) Complete the first endorsement on the request for access form (Appendix A). This will certify the current level of clearance and investigation that the individual requesting access possesses.

(b) Forward the request for access to DC/S PP&O (PL).

Enclosure (1)

1

(3) The DC/S PP&O (PL) will:

(a) Upon receipt of a request for access to SIOP-ESI, complete the access form (Appendix A) requesting security certification from ARFD.

(b) After ARFD certifies the individual's security clearance, brief the individual on the responsibilities of SIOP-ESI access (Appendix B).

(c) Grant access in the appropriate category(ies) (Appendix C).

(d) Maintain the completed access and briefing forms.

(e) Maintain a master OPNAV SIOP-ESI access file.

(f) Ensure that the master access file is updated quarterly.

(g) Distribute quarterly access listings to HQMC staff agencies for review, required action, and concurrence

(h) Debrief personnel whose access is terminated and maintain a file of debriefing certificates.

d. Briefings. Requests for SIOP-ESI briefings for HQMC personnel will be coordinated with DC/S PP&O (PL).

e. Debriefing. When personnel granted access to SIOP-ESI are detached from HQMC or transferred to a billet not requiring SIOP-ESI access, they will be debriefed using the debriefing certificate (Appendix C). It is the responsibility of the heads of staff agencies to ensure that individuals to be debriefed report to DC/S PP&O (PL). For general officers, debriefing will be done at a location and time convenient to the general officer concerned.

3. Duty Assignment and Travel Restrictions. Personnel who have detailed knowledge and continuing access to SIOP-ESI information may be subject to travel and assignment restrictions, as determined by the authority granting access. Restriction determinations will be made as per references (a) and (b). To the extent practicable, personnel who have detailed knowledge and continuing access to SIOP-ESI information should not be assigned to or directed to participate in hazardous activities. Hazardous activities include assignment or travel in combat zones or other areas where hostilities are taking place, exposed areas where individuals cannot reasonably be protected against hostile action, and countries listed in reference (b). Regardless of the degree of access, all personnel who have access to SIOP-ESI must be briefed by the DC/S PP&O (PL) concerning their security responsibilities prior to participation in any hazardous activity or official and unofficial travel through countries posing a security risk. Individuals who frequently travel to said locations shall be provided a thorough briefing at least once each six months.

OPNAV CRST

4. Security of SIOP-ESI Material. All SIOP-ESI material is classified Top Secret. Reference (c) requires that two-person integrity be maintained when Top Secret material is accessible. Only personnel requiring access to SIOP-ESI will be granted access to safes containing such material. SIOP-ESI messages must be processed as "Special Category" messages per NTP4. References (a) and (b) specify the requirements for personnel who act as couriers for SIOP-ESI information.

5. Destruction. HQMC staff agencies which receive SIOP-ESI materials will return these materials to DirAR (ARFD) for destruction when they are no longer required for operational use or no more than 30 days after supersession. Enclosure (1)

MCO 5511.18A
30 Oct 98

Sample Request for Access to SIOP-ESI

PLN-8
30 October, 1998

From: National Plans Branch, Plans Division
To: PP&O SIOP Control Officer
Via: Director of Administration and Resources Management (ARFD)

Subj: REQUEST FOR ACCESS TO SIOP-ESI

Ref: (a) OPNAVINST S5511.35K

1. It is requested that the following individual, certified to have a "need to know" in accordance with the reference, be granted access to SIOP-ESI for the categories listed below:

Name (Last, First MI) Rank/GS SSN Office *Cat*

Date of birth: Place of birth:

(Branch Chief, National Plans Branch)
Colonel, U.S. Marine Corps

* Categories in Annex A to enclosure (1) of reference (a).

FIRST ENDORSEMENT _____
(Date)

From: Director of Administration and Resources Management (ARFD)
To: PP&O SIOP Control Officer

1. The above named applicant for SIOP-ESI access is certified to possess a FINAL TOP SECRET clearance. Additionally, an SBI has been completed/initiated as indicated below.

SBI initiated on _____ SBI completed on _____ by _____
BI completed on _____ by _____ (waiver requested)

(Signature of Security Officer)

Appendix A

1

MCO 5511.18A
30 Oct 98

STATEMENT OF ACKNOWLEDGEMENT OF ACCESS TO SIOP-ESI

I acknowledge that I will be authorized access to information contained in the Single Integrated Operational Plan (SIOP) and certain annexes, thereto, which contain Extremely Sensitive Information (ESI) in the following category:

I have read and understand the instructions and procedures contained in the current OPNAVINST S5511.35 and that when a change in my assignment or any other change in my status no longer required access to SIOP-ESI, I will execute the debriefing certificate.

I understand that the security of SIOP-ESI is of paramount importance and that its compromise could cause exceptionally grave damage to the United States.

In witness, thereof, I do solemnly certify that I will not discuss with or disclose to any person SIOP-ESI information, or that I have an SIOP-ESI access, unless that person is currently authorized access to such information, and then only when required by my duty assignment.

Signed this date, the ____ day of _____, 19__.

(Signature of Individual)

(Signature/Rank/N Code of Witness)

DEBRIEFING STATEMENT

I am aware that I am no longer authorized access to SIOP-ESI information. Pursuant to the obligation I incurred, at the time and place I was authorized access to SIOP-ESI, I reaffirm that at no time will divulge or discuss SIOP-ESI information unless required to do so by competent authority.

(Signature of Individual) (Date)

(Signature/Rank/N Code of Witness) (Date)

Appendix B

1

Page 7

MCO 5511.18A
30 Oct 98

Subj: REQUEST FOR ACCESS TO SIOP-ESI

SECOND ENDORSEMENT _____
(Date)

From: PP&O SIOP Control Officer

1. Access to SIOP-ESI information is granted/not granted.

(SIOP CONTROL OFFICER)
Lieutenant Colonel, U. S. Marine Corps

Appendix C

1