



UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN), FMF

UNIT 35801

FPO AP 96602-5801

DivO P5510.9K

SECMGR

6 Apr 93

DIVISION ORDER P5510.9K

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR IPSP)

Encl: (1) LOCATOR SHEET

1. Purpose. To publish standing operating procedures for the Information and Personnel Security Program within the 3d Marine Division.
2. Cancellation. DivO P5510.9J and DivO P5511.6.
3. Scope. This Order, used in conjunction with the references, provides policy, procedures, and other amplifying information necessary for the operation of the subject program.
4. Action. Regiments, Headquarters Battalion and separate battalions will not publish directives covering this subject. UDP battalions will not publish directives covering this subject, or use similar directives from organizations other than the 3d Marine Division. If commanding officers desire to impose more stringent requirements within their command, they may add an additional chapter to this SOP.
5. Summary of Revision. This revision contains a substantial number of changes and should be completely reviewed.
6. Recommendations. Recommendations for improving this directive are actively solicited. Such recommendations will be forwarded to this Headquarters (Security Manager) via the appropriate chain of command.
7. Certification. Reviewed and approved this date.

R. A. HORD
Chief of Staff

DISTRIBUTION: A/D



UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN), FMF
UNIT 35801
FPO AP 96502-5801

DivO P5510.9K
SECMGR
6 Apr 93

DIVISION ORDER P5510.9K

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR IPSP)

Encl: (1) LOCATOR SHEET

1. Purpose. To publish standing operating procedures for the Information and Personnel Security Program within the 3d Marine Division.
2. Cancellation. DivO P5510.9J and DivO P5511.6.
3. Scope. This Order, used in conjunction with the references, provides policy, procedures, and other amplifying information necessary for the operation of the subject program.
4. Action. Regiments, Headquarters Battalion and separate battalions will not publish directives covering this subject. UDP battalions will not publish directives covering this subject, or use similar directives from organizations other than the 3d Marine Division. If commanding officers desire to impose more stringent requirements within their command, they may add an additional chapter to this SOP.
5. Summary of Revision. This revision contains a substantial number of changes and should be completely reviewed.
6. Recommendations. Recommendations for improving this directive are actively solicited. Such recommendations will be forwarded to this Headquarters (Security Manager) via the appropriate chain of command.
7. Certification. Reviewed and approved this date.

R. A. HORD
Chief of Staff

DISTRIBUTION: A/D



OFFICIAL FILE COPY
UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN), FMF
UNIT 35801
FPO AP 96602-5801

Divo P5510.9K Ch 1
SECMGR
11 May 93

DIVISION ORDER P5510.9K Ch 1

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR IPSP)

Encl: (1) New page insert to Divo P5510.9K

1. Purpose. To transmit new page insert to the basic Manual.

2. Action.

✓ a. Remove pages 16-5, 16-6 and replace them with the
corresponding pages contained in the enclosure hereto.

3. Summary of Changes. To update information contained in the
basic Manual.

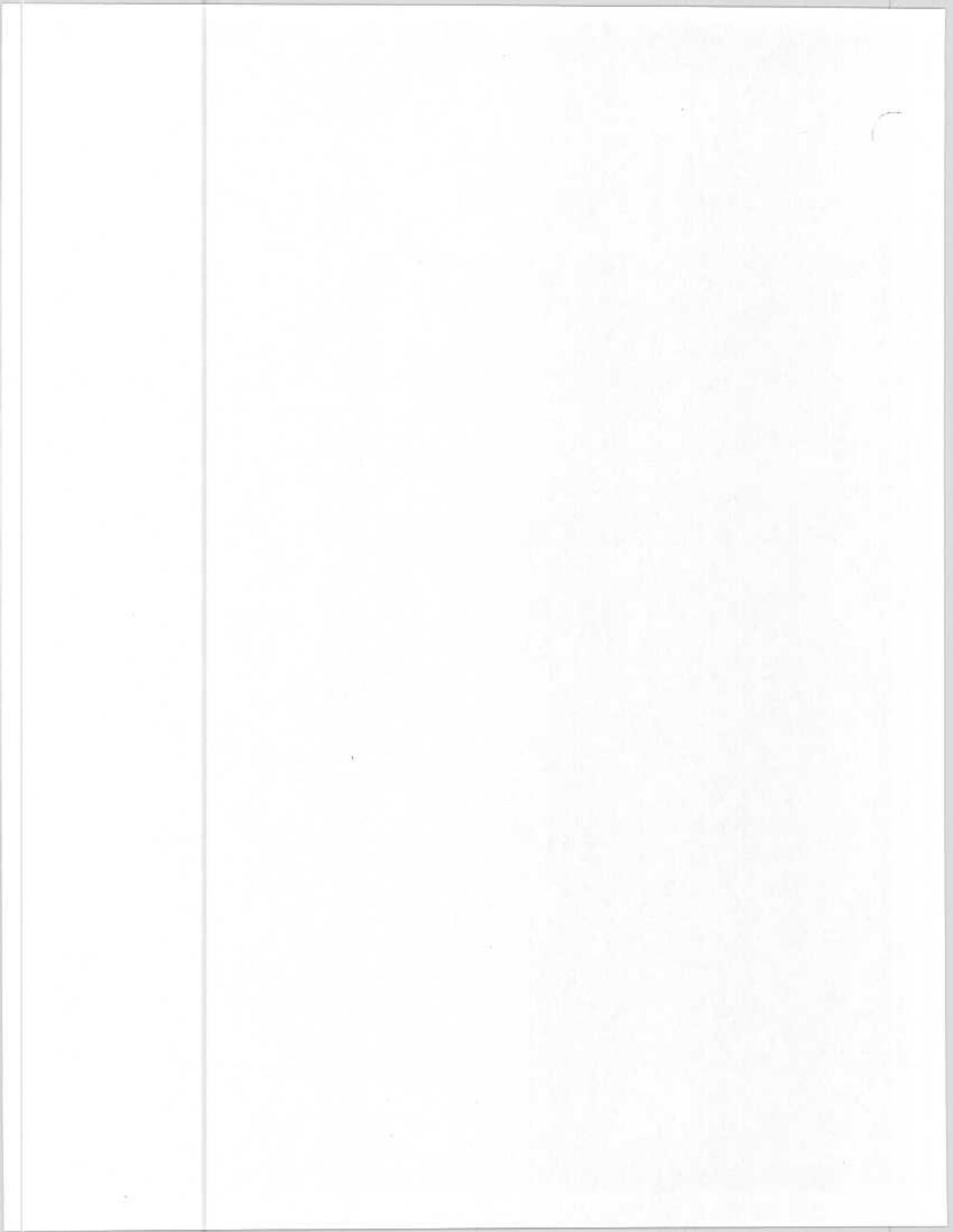
4. Change Notation. Significant changes contained in the revised
pages for this Change are denoted by an arrow (→) symbol.

5. Filing Instructions. This Change transmittal will be filed
immediately following the signature page of the basic Manual

6. Certification. Reviewed and approved this date.

R. A. HORD
Chief of Staff

DISTRIBUTION: A/D



DivO P5510.9K
6 Apr 93

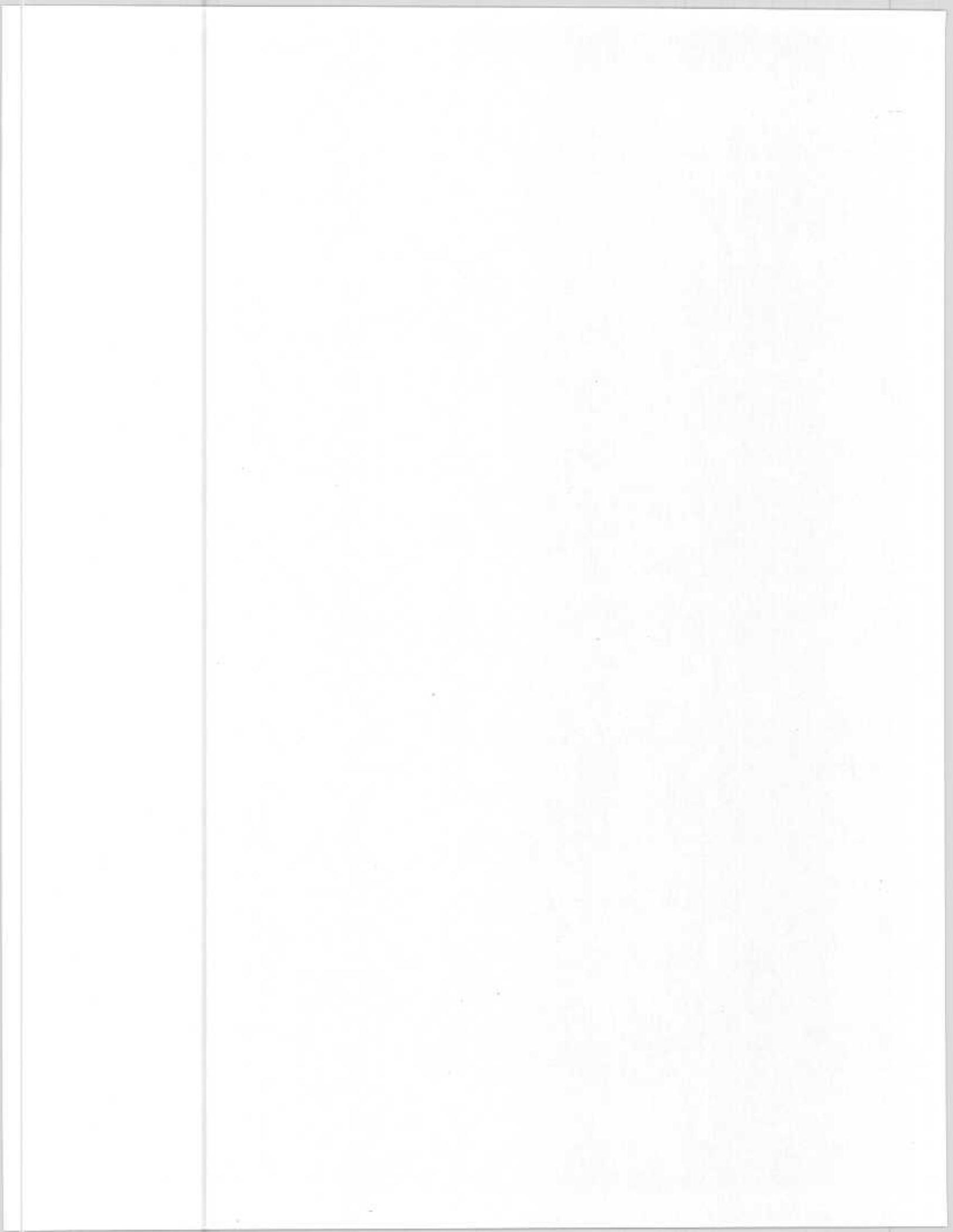
LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR IPSP)

Location: _____

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

ENCLOSURE (1)

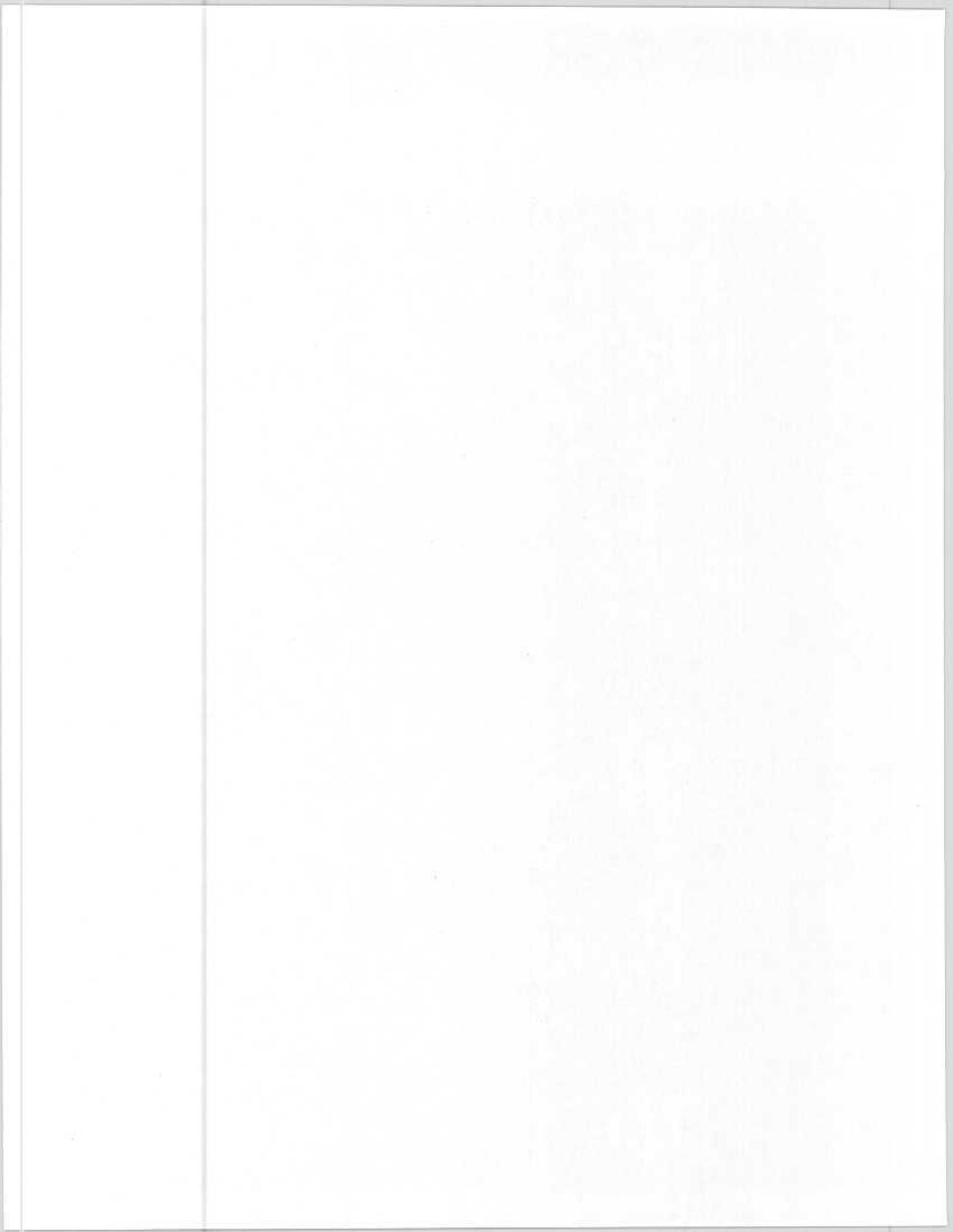


SOP FOR IPSP

RECORD OF CHANGES

Log completed change action as indicated.

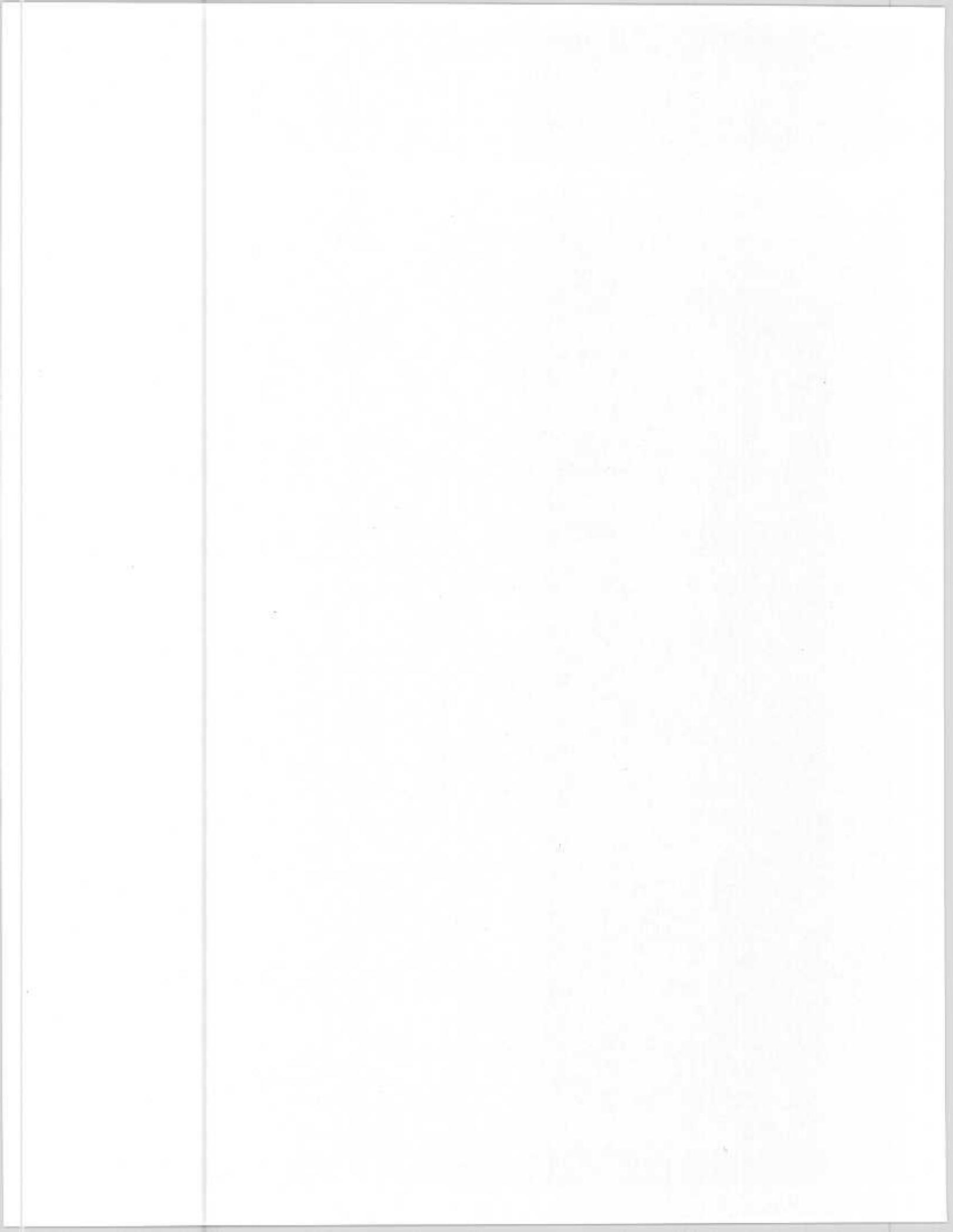
Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change
1	11 May 93	13 May 93	13 May 93	Tommy S. Phillips LCpl



SOP FOR IPSP
TABLE OF CONTENTS

CHAPTER

1	GENERAL
2	PROGRAM MANAGEMENT
3	SECURITY EDUCATION
4	COMPROMISE AND OTHER SECURITY VIOLATIONS
5	COUNTERINTELLIGENCE MATTERS TO BE REPORTED
6	CLASSIFICATION
7	CLASSIFICATION GUIDES
8	DECLASSIFICATION, DOWNGRADING AND UPGRADING
9	MARKING
10	ACCOUNTING AND CONTROL
11	PRINTING, REPRODUCTION AND PHOTOGRAPHY
12	DISSEMINATION OF CLASSIFIED MATERIAL
13	SAFEGUARDING
14	STORAGE
15	TRANSMISSION OF CLASSIFIED MATERIAL
16	HANDCARRYING CLASSIFIED MATERIAL
17	DESTRUCTION OF CLASSIFIED AND UNCLASSIFIED MATERIAL
18	VISITOR CONTROL
19	MEETINGS
20	PERSONNEL SECURITY PROGRAM
21	PERSONNEL SECURITY INVESTIGATIONS
22	PERSONNEL SECURITY DETERMINATIONS
23	CLEARANCE
24	ACCESS



SOP FOR IPSP

TABLE OF CONTENTS

CHAPTER

25 OPTIONAL

APPENDIX

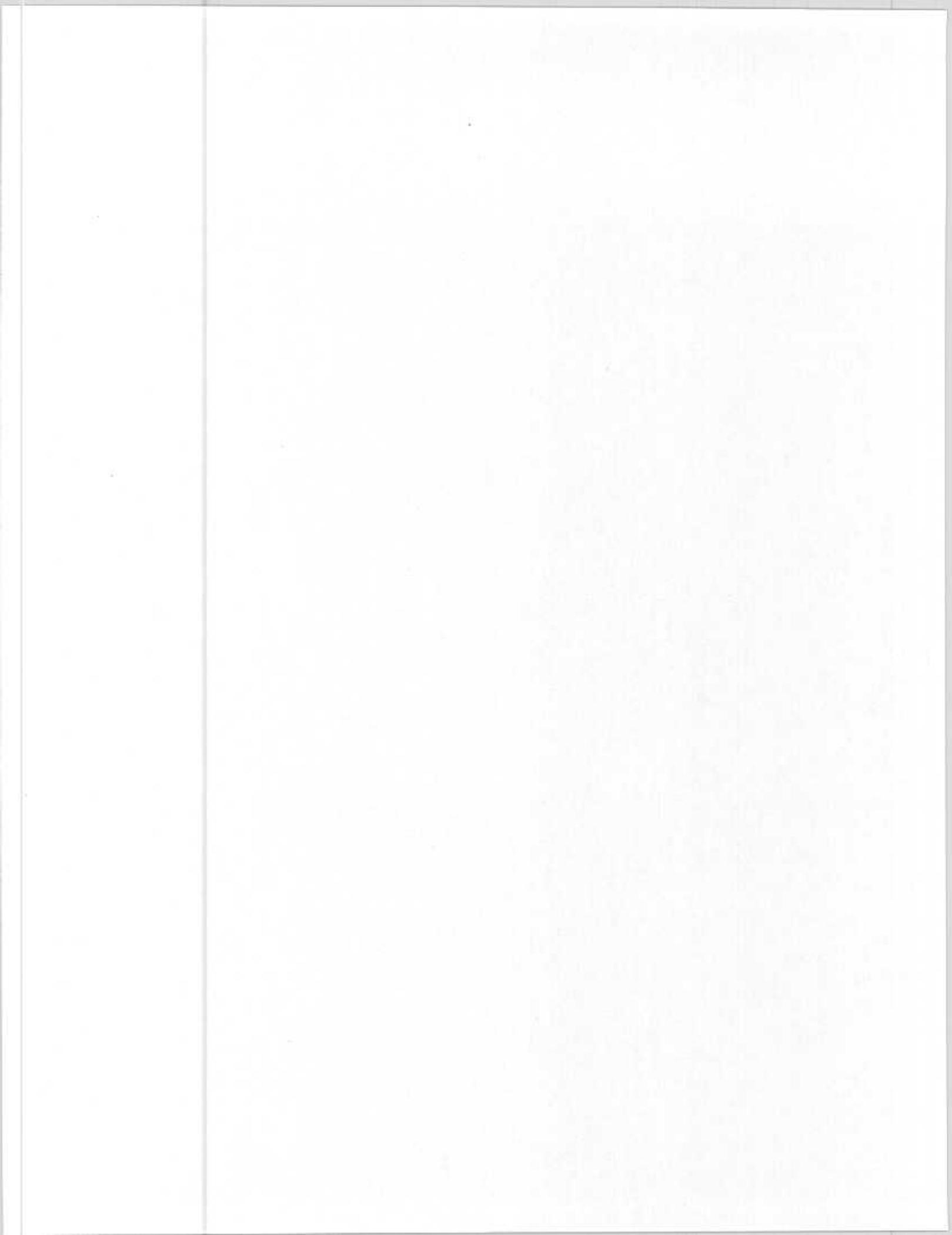
A REFERENCES

SOP FOR IPSP

CHAPTER 1

GENERAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC GUIDANCE.....	1000	1-3
AUTHORITY.....	1001	1-3
APPLICABILITY.....	1002	1-3
RESPONSIBILITY FOR COMPLIANCE.....	1003	1-3
SPECIAL ACCESS PROGRAMS.....	1004	1-3
SENSITIVE COMPARTMENTED INFORMATION.....	1005	1-4
ATOMIC ENERGY ACT.....	1006	1-4
COMBAT OPERATIONS.....	1007	1-4
WAIVERS.....	1008	1-4
ITEMS NOT ADDRESSED.....	1009	1-4



SOP FOR IPSP

CHAPTER 1

GENERAL

1000. BASIC GUIDANCE. Appendix A lists the references used in this regulation. References (a) and (b) provide the basic guidance for the Information and Personnel Security Program within the Department of Defense. References (a) and (b) are supplemented by reference (c), which is the Department of the Navy Information and Personnel Security Program Regulation.

1001. AUTHORITY. The Commanding General is responsible for establishing and maintaining an Information and Personnel Security Program in compliance with the current editions of references (a), (b) and (c). The Command Security Manager is designated as the official primarily responsible for ensuring there is an effective program, and that it complies with all the directives issued by higher authority. The security manager has the full authority of the Commanding General to issue orders and directives relating to the Information and Personnel Security Program.

1002. APPLICABILITY

1. The provisions of this Order are applicable to all general and special staff sections within this headquarters, and all commanding officers and officers in charge of subordinate and attached units.

2. This Order addresses those elements of information and personnel security specifically pertinent to the Division and is intended to be used in conjunction with the current editions of the references.

1003. RESPONSIBILITY FOR COMPLIANCE. Commanding officers, heads of General and Special staff sections, officers in charge and section heads, are responsible for implementation and compliance with this Order. Every Marine, Sailor or civilian attached to the Division is responsible for compliance with this Order and the protection of classified information.

1004. SPECIAL ACCESS PROGRAMS

1. Within the Division, any program requiring additional security measures or special investigative, adjudication or clearance procedures, is considered a special access program.

2. Special access programs, other than those addressed in this Order, will not be established until requested and approved by higher headquarters in accordance with paragraph 1-5 of reference (c).

1005. SENSITIVE COMPARTMENTED INFORMATION. All Sensitive Compartmented Information (SCI) or Special Intelligence (SI) material received, stored, transmitted and destroyed by the 3d Marine Division, will be handled and controlled in accordance with established regulations by the Special Security Office (SSO). Access to this information will also be controlled by the SSO.

1006. ATOMIC ENERGY ACT. The Atomic Energy Act of 30 Aug 1954, as amended, and Department of Energy directives regulate the handling, protection and classification of restricted data and formerly restricted data. The current edition of reference (a) provides guidance for handling this information.

1007. COMBAT OPERATIONS. Security requirements of reference (c) and this Order may be modified as necessary to meet local conditions in combat or combat related operations. Even in those circumstances, follow the provisions of reference (c) and this Order as closely as possible. Training exercises or operations are not considered combat or combat related activities.

1008. WAIVERS. When requirements of reference (c) and this Order result in unacceptable sacrifice of operating efficiency, or when there are other sufficient reasons, a waiver of a specific requirement may be requested. Requests for waivers will be submitted to the Division Security Manager with justification as to why requirements can not be met and describe an alternate procedure. All waivers will be handled on a case-by-case basis.

1009. ITEMS NOT ADDRESSED. Although this Order supplements Information and Personnel Security Program directives, it may not address all areas within the program. Policy and guidance in higher headquarters' directives are of such length and detail that they may not have been incorporated. If guidance on a specific item cannot be found in this Order, consult the identified references and directives. If that fails to answer the question, contact the Division Security Manager.

SOP FOR IPSP
 CHAPTER 2
 PROGRAM MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	2000	2-5
COMMAND RESPONSIBILITY.....	2001	2-5
SECURITY MANAGER.....	2002	2-5
ASSISTANT SECURITY MANAGER.....	2003	2-7
TOP SECRET CONTROL OFFICER/ALTERNATE/ ASSISTANT.....	2004	2-7
CLASSIFIED MATERIAL CONTROL CENTER OFFICER/ASSISTANT/CLERK.....	2005	2-8
SECONDARY CONTROL POINT CUSTODIAN/ ASSISTANT (SCPC/SCPA).....	2006	2-8
SUB-CUSTODY CONTROL POINT CUSTODIAN (SCCPC).....	2007	2-9
CLASSIFIED MATERIAL REPRODUCTION CONTROL OFFICER/ALTERNATE.....	2008	2-9
COMMUNICATIONS SYSTEMS MATERIAL (CMS) CUSTODIAN/ALTERNATE.....	2009	2-9
PERSONNEL RELIABILITY PROGRAM (PRP) CERTIFYING OFFICER.....	2010	2-9
NAVAL WARFARE PUBLICATIONS (NWP) CUSTODIAN.....	2011	2-10
INFORMATION SYSTEMS SECURITY OFFICER (ISSO).....	2012	2-10
SPECIAL SECURITY OFFICER/ASSISTANT (SSO/ASSO).....	2013	2-10
COMMUNICATIONS SECURITY (COMSEC) OFFICER.....	2014	2-11
OPERATIONS SECURITY (OPSEC) OFFICER.....	2015	2-11

SOP FOR IPSP

CHAPTER 2

PROGRAM MANAGEMENT

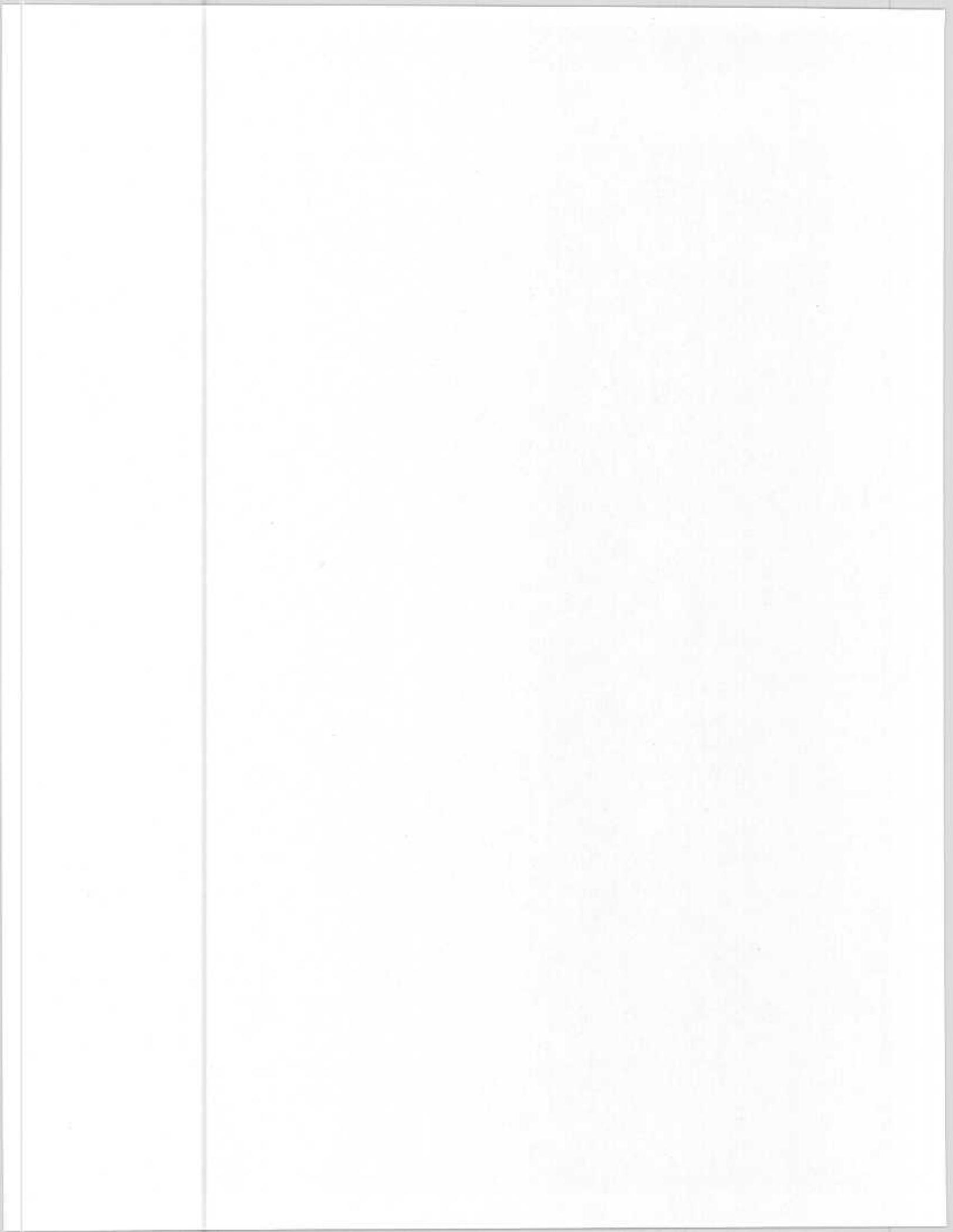
	<u>PARAGRAPH</u>	<u>PAGE</u>
WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM (WWMCCS) AUTOMATED DATA PROCESSING TERMINAL AREA SECURITY OFFICER (WATASO).....	2016	2-11
CLASSIFIED MATERIAL CONTROL CENTER(CMCC)....	2017	2-11
EMERGENCY PLANS.....	2018	2-13
TURNOVER FOLDER/DESKTOP PROCEDURES.....	2019	2-14
INSPECTIONS.....	2020	2-14
UNANNOUNCED AFTER HOURS SECURITY INSPECTION.....	2021	2-15
ENTRANCE AND EXIT SECURITY INSPECTION.....	2022	2-15
INFORMATION SYSTEMS SECURITY INSPECTION.....	2023	2-16
OTHER INSPECTIONS.....	2024	2-16
PHYSICAL SECURITY EVALUATION.....	2025	2-16

FIGURE

2-1	SECURITY MANAGER/ASSISTANT APPOINTMENT LETTER.....	2-18
2-2	TOP SECRET CONTROL OFFICER/ALTERNATE APPOINTMENT LETTER.....	2-19
2-3	CLASSIFIED MATERIAL CONTROL CENTER OFFICER/ASSISTANT APPOINTMENT LETTER..	2-20
2-4	SECONDARY CONTROL POINT CUSTODIAN/ ASSISTANT APPOINTMENT LETTER.....	2-21
2-5	SUB-CUSTODY CONTROL POINT CUSTODIAN APPOINTMENT LETTER.....	2-22
2-6	CLASSIFIED MATERIAL REPRODUCTION CONTROL OFFICER/ALTERNATE APPOINTMENT LETTER..	2-23

SOP FOR IPSP
CHAPTER 2
PROGRAM MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
2-7	INFORMATION SYSTEMS SECURITY OFFICER/ ASSISTANT APPOINTMENT LETTER.....	2-24
2-8	SPECIAL SECURITY OFFICER/ASSISTANT....	2-25
2-9	UNANNOUNCED AFTER HOURS SECURITY INSPECTION REPORT.....	2-26
2-10	ENTRANCE AND EXIT SECURITY INSPECTION REPORT.....	2-27
2-11	INFORMATION SYSTEMS SECURITY INSPECTION REPORT.....	2-28



SOP FOR IPSP

CHAPTER 2

PROGRAM MANAGEMENT

2000. BASIC POLICY. Commanding officers, General and Special staff officers, officers in charge, and section heads are responsible for safeguarding all classified information within their command/section and ensuring that all personnel receive instruction on current security practices and procedures.

2001. COMMAND RESPONSIBILITY

1. The Commanding General/commanding officers are responsible for effective management of the Information and Personnel Security Program within their commands.

2. Command security management, discussed in detail in subsequent paragraphs, includes:

- a. Designating a security manager.
- b. Designating a top secret control officer.
- c. Designating an ADP Security Officer (or Information Systems Security Officer) if the command processes data or prepares documents on automated systems.
- d. Preparing written command security procedures.
- e. Preparing an emergency action plan for the protection of classified material.
- f. Reviewing and inspecting the effectiveness of the program in subordinate commands.

2002. SECURITY MANAGER

1. The Chief of Staff will designate in writing (figure 2-1) the Command Security Manager for the 3d Marine Division. Commanding officers will designate in writing (figure 2-1) a security manager to administer the Information and Personnel Security Program for their unit. Units are strongly encouraged to use signs, photographs or other formats to provide continuous identification of the unit security manager.

2. The security manager must be a U.S. citizen, a commissioned officer with sufficient authority and staff to manage the program, and have been the subject of a satisfactorily adjudicated background investigation (BI).

3. The security manager is the Commanding General/commanding officer's principal adviser and direct representative on information and personnel security matters. He will be

responsible for the following:

a. Guidance, coordination, implementation, and oversight of the Information and Personnel Security Programs.

b. Developing written command information and personnel security procedures.

c. Formulating and coordinating the security education program within the command.

d. Making sure that threats to security, compromises, and security violations are reported, recorded, and when necessary, investigated. Ensure incidents falling under the investigative jurisdiction of the Naval Criminal Investigative Service (NCIS) are immediately referred to the nearest NCIS office, see appendix D of reference (b).

e. Administering the command's program for classification, declassification, and downgrading of classified material.

f. Coordinating the preparation of classification guides for protecting classified material.

g. Coordinating with the unit's Public Affairs Officer to ensure that proposed press releases which may contain classified information are referred to the Security Manager for review.

h. Ensuring compliance with accounting and control requirements for classified material; including, receipt, distribution, inventory, reproduction, and disposition.

i. Formulating and coordinating physical security measures for protecting classified material.

j. Ensuring that any electrical or electronic processing equipment meets control of compromising emanations (TEMPEST) requirements.

k. Ensuring security control of classified visits to and from the command.

l. Ensuring protection of classified information during visits to the command by personnel who do not have clearance or access authorizations.

m. Preparing recommendations for release of classified material to foreign governments. Units of the 3d Marine Division will not release classified material to foreign governments.

n. Ensuring compliance with the industrial security program for classified contracts with Department of Defense contractors.

o. Ensuring that all personnel with access to classified information, or who are assigned to sensitive duties, are appropriately cleared; and that requests for personnel security investigations are properly prepared, submitted and monitored.

p. Ensuring that access to classified material is limited to those with a need-to-know.

q. Ensuring that personnel security investigations, clearances and access are properly recorded.

r. Coordinating the command program for continuing evaluation of eligibility for access to classified information or assignment to sensitive duties.

s. Coordinating with the 3d Marine Division Special Security Office concerning investigations, access to Special Compartmented Information (SCI), continuous evaluation of eligibility, and changes to information and personnel security policies and procedures.

t. Maintaining records of foreign travel reported by assigned personnel. These records should identify, whenever possible, the travelers route and mode of travel, destination, length of stay, identity of fellow travelers (when accompanying the traveler) and tour operator, if a tour operator is used.

u. Coordinate with the command Automated Data Processing and Physical Security Officer on matters of common concern.

2003. ASSISTANT SECURITY MANAGER. The assistant security manager, if assigned, will be designated in writing using the format shown in figure 2-1, and hold the rank of staff sergeant or above. The assistant security manager, if assigned, will assist the security manager with managing the Information and Personnel Security Program and perform all duties of the security manager in the latter's absence. See paragraph 2-11.4 of reference (c) for restrictions concerning enlisted assistant security managers and their authority to issue security clearances for the commander.

2004. TOP SECRET CONTROL OFFICER/ALTERNATE/ASSISTANT

1. Each subordinate unit will designate in writing, a Top Secret Control Officer (TSCO). The format for appointing the TSCO is provided in figure 2-2. For the Division Headquarters, the Adjutant will appoint the TSCO. At the Division Headquarters, the Classified Material Control Center Officer (CMCCO) will be assigned as the alternate TSCO. The Division/unit adjutant will assign Top Secret Control Assistants (TSCA) as necessary using figure 2-2.

2. The person designated as TSCO must be an officer or staff

noncommissioned officer in the grade of gunnery sergeant or above. The TSCO must be a U. S. citizen with a final top secret clearance. The TSCO must be a reliable person with mature judgment. Top secret control assistant(s) will be a U.S. citizen, a sergeant or above and possess a final top secret clearance. Appointment letters for the alternate TSCO and assistant(s) will not include the requirement to inventory all top secret material. The Division/unit security manager will be provided with a copy of all TSCO, alternate TSCO and TSCA appointment letters.

3. The TSCO is responsible to the security manager for the receipt, custody, accountability and disposition of all top secret material in the unit.

4. The TSCO will be guided by the instructions contained in paragraph 2-10 of reference (c) in the performance of his duties. Particular attention must be given to the requirement that top secret material be transmitted by direct personal contact using a continuous chain of signed receipts and disclosure records.

2005. CLASSIFIED MATERIAL CONTROL CENTER OFFICER (CMCCO)/ASSISTANT

1. The CMCCO will be appointed in writing using the format shown in figure 2-3. The CMCCO will be a warrant officer or above with the investigative basis and security clearance commensurate with the levels of classified material maintained by the unit. The assistant CMCCO will be a staff sergeant or above with at least a secret clearance. CMCC clerks may be assigned by the Division or unit adjutant as necessary. CMCC clerks may be of any rank with at least a secret clearance. Appointment letters for the assistant CMCCO and clerks will not include the requirement to inventory classified material held by the CMCC. The Division/unit security manager will be provided with a copy of all CMCC related appointment letters.

2. The CMCCO is responsible for the accountability and control of all classified material received, held, originated, transferred or destroyed by the unit per reference (c) and this Order.

2006. SECONDARY CONTROL POINT CUSTODIAN/ASSISTANT (SCPC/SCPA)

1. Security managers will appoint SCP custodians in writing using the format shown in figure 2-4. Work sections will prepare the appointment letter and submit it to the security manager. For the Division Headquarters, the Division Security Manager will sign SCPC and SCPA appointment letters. The SCPC will be a staff sergeant or above. The SCPA can be any rank and will be assigned in writing using the format shown in figure 2-4. Appointment letters for SCPA(s) will not include the requirement to inventory the classified material held by the SCP.

2. The SCPC will receive, establish control of and administer accounting procedures set forth in reference (c) and this Order for classified material drawn from the unit CMCC and held by the SCP. The SCPA(s) is an administrative assistant to the SCPC.

2007. SUB-CUSTODY CONTROL POINT CUSTODIAN(SCCPC). If necessary, unit security managers may appoint SCCPC using the format in figure 2-5. SCCP's will not be established for the convenience of a particular work section or activity. If deemed necessary, the SCCPC will be a staff sergeant or above. SCCP assistants are not required and will not be assigned.

2008. CLASSIFIED MATERIAL REPRODUCTION CONTROL OFFICER/ALTERNATE

1. The unit classified material reproduction control officer is responsible for approving all requests to reproduce classified material controlled and held by the command. Reproduction control officers are also responsible for ensuring that all reproduction prohibitions are observed, that the reproduction of classified material is kept to an absolute minimum and material reproduced is properly controlled in accordance with reference (c) and this Order. The classified material reproduction control officer and alternate will be assigned in writing by the unit security manager using the format shown in figure 2-6. The unit CMCCO and alternate will normally be assigned this responsibility.

2. Heads of General and Special staff sections, and all major subordinate command (MSC) principle and special staff officers are authorized to approve reproduction of confidential and secret messages only under the conditions listed in paragraph 11000 of this Order.

2009. COMMUNICATIONS SYSTEMS MATERIAL (CMS) CUSTODIAN/ALTERNATE

The CMS custodian is the primary accountant for all CMS material on charge to the Division or subordinate unit CMS account. The CMS custodian will administer the account in accordance with provisions of the current editions of references (d) and (e) and other pertinent CMS directives. Prerequisites for assignment as the custodian/alternate and format for appointment letters are contained in reference (e). Division/unit security managers will be provided with a copy of all CMS related appointment letters. The primary CMS custodian will not be assigned any additional duties within the Information and Personnel Security Program.

2010. PERSONNEL RELIABILITY PROGRAM (PRP) CERTIFYING OFFICER

The Commanding Officer, 12th Marines, is the PRP certifying officer for the Division, and is responsible for the screening and certification of personnel into the Division PRP. The PRP certifying officer will be guided by the current editions of reference (f), Marine Corps Personnel Reliability Program, reference (g), Nuclear Weapons Management Manual, and other

applicable directives.

2011. NAVAL WARFARE PUBLICATIONS (NWP) CUSTODIAN. The NWP custodian, assigned by and under the cognizance of the G-3/S-3, is responsible for the administration and security of the NWP library. The custodian will be guided in the performance of his duties by the current edition of reference (h), Naval Warfare Publications Guide. The G-3/S-3 will ensure a copy of the NWP custodian appointment letter is provided to the Division/unit security manager.

2012. INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

1. The ISSO, under the staff cognizance of the Assistant Chief of Staff, G-6, is responsible to the Division Security Manager for the protection of classified information processed on automated word processing equipment and microcomputers within the Division. The Division Information Systems Management Officer (ISMO) will be assigned duties as the ISSO by the Division Security Manager using the format contained in figure 2-7.

2. The ISSO will publish written guidance for the security of hardware and software as pertains to the security of classified data for the Division.

3. The ISSO will perform his duties and comply with the instructions contained in references (i), (j) and (k).

4. Security managers of MSCs will assign the unit S-6 in writing, as the unit ISSO.

2013. SPECIAL SECURITY OFFICER/ASSISTANT (SSO/ASSO)

1. The Chief of Staff will assign the Assistant Chief of Staff, G-2 as the SSO using the format shown in figure 2-7. The SSO is responsible for the Sensitive Compartmented Information Facility (SCIF) and the security, control, dissemination, utilization and destruction of all SCI material.

2. The SSO is responsible for the overall administration of SCI programs. Actual day-to-day functions will be handled by the ASSO. The assignment as ASSO is an additional duty for the Team Commander, 1st Special Security Communications Team (1st SSCT). He will also be assigned in writing by the Chief of Staff using the format shown in figure 2-7.

3. The administrative section of the SSO is responsible for initiating Single-Scoped Background Investigations (SSBI) for personnel requiring SCI access. The administrative section of the SSO will keep appropriate unit security managers apprised on the status and results of all SSBIs for SCI access related to members of their unit.

4. The administrative section of the SSO will provide a copy of all initiated SSBIs for SCI access, to the appropriate unit security manager for inclusion in the subject's official personnel file.

2014. COMMUNICATIONS SECURITY (COMSEC) OFFICER. The Assistant Chief of Staff, G-6, is responsible for the aspects of communications security for the Division. Within subordinate units, the communications officer is responsible for communications security (COMSEC). COMSEC officers will be guided in the performance of their duties by references (l) and (m).

2015. OPERATIONS SECURITY (OPSEC) OFFICER. The operations security officer under the cognizance of the Assistant Chief of Staff, G-3/S-3, is responsible for ensuring security of military operations conducted by or associated with the unit. OPSEC officers are responsible for preparing orders, directives and reports in accordance with references (n) and (o). The OPSEC officer will chair a permanent or ad hoc OPSEC working group consisting of representatives from each staff functional area, to oversee and coordinate the units OPSEC program. The OPSEC officer with the assistance of working group members will formulate and publish classification guidance for operation/exercise plans, systems, programs or projects involving classified material or information per chapter 7 of reference (c) and other applicable directives.

2016. WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM (WWMCCS) AUTOMATED DATA PROCESSING TERMINAL AREA SECURITY OFFICER (WATASO)

1. The WATASO, under the staff cognizance of the Assistance Chief of Staff, G-3, is responsible for the operation of all WWMCCS classified communications and associated material. The WATASO and assistants will be appointed in writing by the Assistant Chief of Staff, G-3, per reference (p). The Division Security Manager will be provided with a copy of all WWMCCS associated appointment letters.

2. The WATASO and assistants will be guided in the performance of their duties by references (p) and (q). WWMCCS products removed from the WWMCCS vault will be protected and controlled per reference (c) and paragraph 10016 of this Order.

2017. CLASSIFIED MATERIAL CONTROL CENTER (CMCC)

1. The Division Headquarters, regiments, separate battalions and UDP battalions, will establish a centralized Classified Material Control Center (CMCC). The CMCC will administer and control all classified material received, held, originated, transferred or destroyed by the command. The unit CMCC also maintains control and accountability for all classified material routed within the command (less SCI material and secret/confidential messages received via servicing communications facilities).

2. The unit CMCC may be established only after the following procedures are completed.

a. A written request to establish a CMCC is submitted to the unit security manager. The request will specify the proposed location of the CMCC, the quantity and classification of the material to be stored therein, and security equipment to be utilized.

b. The unit security manager will conduct a Physical Security Evaluation (PSE) of the proposed CMCC location, and associated security equipment to be utilized for the storage of classified material. Storage criteria outlined in chapter 14 of reference (c), will be used to judge the location and equipment of the proposed CMCC.

c. Should the proposed location meet the security criteria outlined in chapter 14 of reference (c), for a CMCC, the security manager will cause a PSE report to be prepared so stating. The PSE will be endorsed by the unit commanding officer or security manager authorizing the location to be utilized as a CMCC.

d. Should the proposed location not meet the security criteria outlined in chapter 14 of reference (c), because of building structural shortcomings, or insufficient storage equipment, the space will not be authorized to function as a CMCC. As soon as structural modifications are completed or additional security equipment is acquired, the space may be authorized to function as a CMCC.

3. For Unit Deployment Program (UDP) units the following procedures will apply. The unit security manager departing will conduct a turnover with the incoming security manager. CMCC and SCP spaces will be inspected and a determination made that all security criteria addressed in the current PSE remains the same (i.e., space, safes, quantity/classification of material to be stored). If the PSE is still valid, the new unit security manager will attach a new endorsement to the PSE authorizing the space to be utilized as a CMCC/SCP.

4. A PSE remains valid until a change in security equipment or a structural change to the space occurs. The exception to this policy is CMS spaces. A PSE for CMS spaces will be revalidated every 18 months per references (d) and (e).

5. Headquarters Battalion will not establish a CMCC. Headquarters Battalion will be designated as an SCP and draw classified material from Division CMCC, as required.

6. Secondary Control Points (SCP). SCPs may be established when work sections cannot conveniently store classified material within the unit CMCC. The criteria for establishing an SCP is the same as that for establishing a CMCC. An SCP will draw classified

material from that units CMCC only. An SCP is not authorized to pass classified material to another SCP and bypass the unit CMCC.

7. Sub-Custody Control Point (SCCP). SCCPs may be established for a work section when classified material cannot be conveniently stored within the section's SCP. The criteria for establishing a SCCP is the same as that for establishing a CMCC. A SCCP will only draw and return classified material from its work section SCP. Careful consideration will be given to the establishment of any SCCP. Proper security and storage of the classified material should be considered first, over convenience for the work section. The primary reason for establishment of a SCCP, will be due to part of a work section being physically located in an adjacent building, not an adjacent office.

8. Storage for classified material, of any level of classification, is not authorized in spaces which are not designated as a CMCC, SCP or SCCP. Acquisition of a GSA approved security container is not authorization to store classified material.

9. On occasion, work sections that do not have an SCP, may generate classified material to support operations and exercises of the unit. Unit security managers must decide whether that section will be required to store the material in the unit CMCC, or establish an SCP without authorization to draw classified material from the CMCC.

2018. EMERGENCY ACTION PLANS (EAP). Security managers will ensure that every unit/section authorized to store classified material will develop an EAP for the protection, removal or destruction of classified material in the event of natural disaster, civil disorder or enemy action. The CMCC officer, in coordination with the adjutant, will develop and prepare a letter type EAP directive for the unit. Work sections with an SCP are required to prepare an EAP that specifically addresses classified material held by that section. Work section/SCP EAPs will be coordinated with the units overall plan.

1. Security managers will ensure that each unit/section EAP is tested at least once each year, or once each deployment (within 60 days of main body arrival) for UDP units. Personnel who participate in the drill should be properly cleared (appropriate clearance and access) but not familiar with CMCC/CMS/SCP procedures to ensure realistic results/evaluation of the plan. CMCC/CMS/SCP custodians will participate in the drill as evaluators only, to ensure that classified material is not lost or inadvertently destroyed.

2. The results of the EAP drill will be recorded and submitted to the unit security manager. Reports will include problems identified and the action taken to resolve them. EAP reports will be retained for two years by the unit security manager and the CMCC officer. For the Division Headquarters and Headquarters

Battalion, EAP drill reports will be submitted to the Division Security Manager with a copy to the Division CMCC Officer.

2019. TURNOVER FOLDER/DESK TOP PROCEDURES

1. Security managers will ensure that turnover folders/desktop procedures are maintained by all personnel who are appointed to a position related to the Information and Personnel Security Program per reference (r).
2. Contents of turnover folders/desktop procedures will include, but are not limited to the following items:
 - a. Appropriate appointment letter(s).
 - b. Appropriate Physical Security Evaluation (PSE) and authorization letters for CMS/CMCC/SCP/SCCP spaces.
 - c. Latest report of unannounced security inspection(s).
 - d. Results of latest Information and Personnel Security Program inspection (Security manager only).
 - e. Unit EAP directive and supporting EAP instructions for CMCC/SCP, as appropriate.
 - f. Detailed administrative instructions for the protection, control, marking, storage and destruction of classified material.

2020. INSPECTIONS

1. All units of the Division are subject to an annual inspection, to evaluate the unit's compliance with the Information and Personnel Security Program. These inspections will normally coincide with Administrative Readiness Evaluations (ARE) and Staff Assistants Visits (SAV) addressed in reference (s).
2. Commanding officers will initiate an internal inspection program of subordinate units/sections. The inspections, utilizing Exhibit 2C of reference (c), will be self-evaluations of the unit's security program management procedures, accounting and control procedures for classified information, physical security, personnel security and security education functions. Results of these self-evaluations will be maintained by the unit security manager.
3. Formal inspections of Unit Deployment Program (UDP) battalions are not required while on Okinawa. Regimental commanders will schedule and conduct a SAV for UDP battalions within 30 days of main body arrival, to ensure the unit's Information and Personnel Security Program is in compliance with reference (c) and this Order.

2021. UNANNOUNCED AFTER HOURS SECURITY INSPECTION

1. Unit security managers will initiate a monthly unannounced after hours security inspection of all sections within their unit that work with or store classified material. These inspections shall determine whether classified material is being properly secured and if administrative requirements, (i.e., security container double check sheets, activity security check sheets) are being utilized properly. A report of the inspection(s) will be prepared and submitted to the unit commander by the security manager. Figure 2-9 will be submitted to the Division Security Manager by the 10th day of the month, detailing the results of the previous months inspection(s). UDP battalion reports will be submitted to the Division Security Manager via the administrative chain of command. The Division Security Manager will conduct unannounced after hours security inspections of the Division's general and special staff sections.

2. The Division Security Manager will direct periodic unannounced security inspections of all sections of the Division Headquarters and subordinate units. These inspections will be conducted by counterintelligence (CI) personnel to determine compliance with physical security requirements and accounting and control of classified material. All CI personnel possess a final top secret clearance. CI personnel will present U.S. Marine Corps CI credentials upon request. Organizational and unit orders for duty personnel will include instructions stating that CI credentials are the only identification required, and that they will be honored as certification of a top secret clearance and access, and constitute a valid "Need-to-Know" for those CI personnel conducting the inspection. Unannounced inspections by CI personnel are designed to supplement, not replace, similar in-house inspections by security program management personnel of the unit.

2022. ENTRANCE AND EXIT SECURITY INSPECTION

1. Unit commanders will implement an Entrance and Exit Security Inspection Program of all personnel entering or exiting their headquarters building(s). The inspection's primary purpose is to ensure that classified material is not being removed or introduced to the unit in violation of the procedures contained in reference (c) and this Order. Articles to be searched during this inspection include, but are not limited to, briefcases, unsealed courier pouches, gym bags, backpacks, etc.. Unit security managers should review Exhibit 13D of reference (c) regarding authority to conduct checks of personal articles to ensure compliance with security regulations.

2. During the inspection, inspectors will ensure that classified material is being wrapped, transported and protected in accordance with security regulations. Inspectors will also ensure that personnel transporting classified material outside headquarters

buildings have been granted the appropriate level security clearance, access and have a valid courier card in their possession.

3. This inspection will be conducted at least once each quarter. A report of the inspection(s) will be prepared and submitted to the unit commander by the security manager. Figure 2-10 will be submitted to the Division Security Manager by the 10th day of the month, detailing the results of the previous quarters inspection(s). UDP battalion reports will be submitted to the Division Security Manager via the administrative chain of command. The Division Security Manager will conduct Random Entrance and Exit Security inspections for the Division Headquarters.

2023. INFORMATION SYSTEMS SECURITY INSPECTION

1. Information systems security officers will conduct a monthly (during working hours) inspection of all work sections that utilize word processing equipment, microcomputers, associated hardware and software. The inspection will determine if work sections are in compliance with security procedures contained in references (c), (i), (j), (k) and this Order.

2. The Division ISSO will conduct this inspection for all General and Special staff sections of the Division Headquarters.

3. A report of the inspection(s) will be prepared and submitted to the Division/unit security manager. Figure 2-11 will be submitted to the Division Security Manager by the 10th day of the month, detailing the results of the previous months inspection(s). UDP battalion reports will be submitted to the Division Security Manager via the administrative chain of command.

2024. OTHER INSPECTIONS. In addition to those inspections contained in the preceding paragraphs, subordinate units are subject to inspections of their Naval Warfare Publications Libraries (NWPL), Classified Material Control Centers, and Communications Security Material System (CMS) account by personnel from the Division Headquarters. These inspections frequently overlap into some of the areas covered by the Information and Personnel Security Program inspections, and will contribute to the overall security posture of the unit.

2025. PHYSICAL SECURITY EVALUATION (PSE). Unit security managers will ensure that a PSE is conducted for any space intended to be designated and utilized for classified material storage.

1. A PSE will be conducted and a report prepared for spaces such as CMS vaults, WWMCCS vaults, CMCCs, SCPs and SCCPs. Security criteria contained in chapter 14 of reference (c) will be followed when inspecting areas and preparing reports for these spaces. CMS spaces will be inspected and reports prepared in accordance with the criteria contained in references (d) and (e). WWMCCS spaces

will be inspected and reports prepared in accordance with the criteria contained in references (p) and (q).

2. At a minimum, a PSE will include the information listed below. Additional information will be included in the PSE when directed by the references associated with the type of space being established.

a. Building number, office/room number, floor of building where space is located and structural description of space (i.e., 8 inch reinforced concrete walls, ceiling and floor).

b. Number of security containers, further identified by manufacturer, number of drawers, model number, class and serial number.

c. Installation where building is located and location of supporting guard force/duty personnel, and whether they are armed.

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Chief of Staff/Commanding Officer

To: Rank, name, SSN/MOS, USMC

Subj: APPOINTMENT AS SECURITY MANAGER

Ref: (a) OPNAVINST 5510.1H

(b) DivO P5510.9K

1. You are appointed as the Security Manager for command/unit in accordance with the references.

2. You will be governed in the performance of your duties by the provisions of the references and other applicable directives. You are directed to thoroughly familiarize yourself with paragraph 2-8 of reference (a).

3. All previous Security Manager appointments are cancelled.

4. You will indicate by endorsement hereon that you have familiarized yourself with paragraph 2-8 of reference (a) and that you have assumed all duties as the Security Manager.

SIGNATURE

FIRST ENDORSEMENT

(DATE)

From: Rank, Name, SSN/MOS USMC

To: Chief of Staff/Commanding Officer

1. I have read and understand the contents of the references and have assumed the duties as the Security Manager.

SIGNATURE

Figure 2-1. Security Manager/Assistant Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Chief of Staff/Commanding Officer
To: Rank, Name, SSN/MOS, USMC
Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER
Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. You are appointed as the Top Secret Control Officer for this command/unit in accordance with the references. You will be governed in the performance of your duties by the provisions of the references and other applicable directives. You are directed to thoroughly familiarize yourself with paragraph 2-10 of reference (a).

3. You will inventory all material in the account, indicate by endorsement hereon, acceptance of the duties and note any discrepancies discovered during your inventory.

SIGNATURE

Copy to:
CMCCO, Sec Mgr, Comm Cntr

FIRST ENDORSEMENT

(DATE)

From: Rank, Name, SSN/MOS, USMC
To: Chief of Staff/Commanding Officer

1. I have familiarized myself with the references, and have assumed all duties as the Top Secret Control Officer.

2. An inventory of all Top Secret material held by this command/unit was conducted on (date). The following discrepancies exist. (or) No discrepancies exist.

SIGNATURE

Figure 2-2. Top Secret Control Officer/Alternate Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Assistant Chief of Staff, G-1/Commanding Officer
To: Rank, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS CLASSIFIED MATERIAL CONTROL CENTER OFFICER

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. You are appointed as the Classified Material Control Center Officer for this command/unit in accordance with the references.
2. You will be governed in the performance of your duties by the provisions of the references and other applicable directives.
3. You and the CMCC Officer you are relieving, will inventory all classified material held by the Classified Material Control Center and all Secondary Control Points (less Top Secret material).
4. You will indicate by endorsement hereon acceptance of the duty assigned and note any discrepancies identified during your inventory.

SIGNATURE

Copy to:
Div Adj, Sec Mgr

FIRST ENDORSEMENT

(DATE)

From: Rank, Name, SSN/MOS, USMC
To: Assistant Chief of Staff, G-1/Commanding Officer

Encl: (1) Inventory

1. I certify that I have completed all relief/turnover requirements, including an inventory of all classified material held by this command. The following discrepancies exist. (or) No discrepancies exist.

SIGNATURE

Figure 2-3. Classified Material Control Center Officer/
Assistant Appointment Letter

SOP FOR IPSP

HEADING

5510 ID
SYMBOL
(DATE)

From: Security Manager
To: Rank, Name, SSN/MOS, USMC
Subj: APPOINTMENT AS SECONDARY CONTROL POINT CUSTODIAN
Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. You are appointed as the Secondary Control Point (SCP) Custodian for the (section) in accordance with the references. You will be guided in the performance of your duties by references (a) and (b).
2. You and the SCP Custodian you are relieving, will inventory all classified material held by the SCP. You will indicate by endorsement hereon, acceptance of the duty assigned and note any discrepancies identified during your inventory.

SIGNATURE

FIRST ENDORSEMENT (DATE)

From: Rank, Name, SSN/MOS, USMC
To: Security Manager

Encl: (1) Inventory

1. I have familiarized myself with the references and have assumed all duties as the (section) SCP Custodian.
2. The enclosure is an inventory of all classified material held by the SCP. The following discrepancies exist (or) No discrepancies exist.

SIGNATURE

Copy to:
CMCC

Figure 2-4. Secondary Control Point Custodian/Assistant Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

FROM: Security Manager
To: Rank, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS SUB-CUSTODY CONTROL POINT CUSTODIAN

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.1K

1. You are appointed as the Sub-Custody Control Point (SCCP) Custodian for (section) in accordance with the references.
2. You will be guided in the performance of your duties by the references and your parent Secondary Control Point (SCP) Custodian. You are authorized to draw classified material from your parent SCP and return it to the same SCP only.
3. You will indicate by endorsement hereon acceptance of the duty assigned.

SIGNATURE

Copy to:
CMCC
SCP Custodian

(DATE)

FIRST ENDORSEMENT

From: Rank, Name, SSN/MOS, USMC
To: Security Manager

1. I have familiarized myself with the references and have assumed the duty assigned.

SIGNATURE

Figure 2-5. Sub-Custody Control Point Custodian Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Security Manager
To: Rank, Name, SSN/MOS, USMC
Subj: APPOINTMENT AS CLASSIFIED MATERIAL REPRODUCTION CONTROL
OFFICER
Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. You are appointed as the Classified Material Reproduction Control Officer for this command/unit in accordance with the references.
2. You will be governed in the performance of your duties by the provisions of the references and other applicable directives.
3. You will indicate by endorsement hereon acceptance of the duty assigned.

SIGNATURE

Copy to:
CMCCO

FIRST ENDORSEMENT

(DATE)

From: Rank, Name, SSN/MOS, USMC
To: Security Manager

1. I have familiarized myself with the references and have assumed the duty assigned.

SIGNATURE

Figure 2-6. Classified Material Reproduction Control Officer/Alternate Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Security Manager
To: Rank, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS INFORMATION SYSTEMS SECURITY OFFICER

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K
(c) DivO P5230.1

1. Per reference (a) and (b), you are appointed as the Information Systems Security Officer for this command/unit.
2. You will be guided in the performance of your duties by the provisions of reference (a) through (c), and other applicable directives.
3. You will indicate by endorsement hereon that you have familiarized yourself with the references and that you have assumed the duty assigned.

SIGNATURE

Copy to:
AC/S, G-6

FIRST ENDORSEMENT

(DATE)

From: Rank, Name, SSN/MOS, USMC
To: Security Manager

1. I have familiarized myself with the references and have assumed the duty assigned.

SIGNATURE

Figure 2-7. Information Systems Security Officer Appointment Letter

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Commanding General

To: Rank, Name, SSN/MOS, USMC

Subj: DESIGNATION AS 3D MARINE DIVISION SPECIAL SECURITY OFFICER

Ref: (a) DoD Dir TS-5105.21-M-2

(b) DoD Dir C-5105.21-M-1

(c) DoD Dir C-5105.21-M-1, Navy Supplement

1. Per the references, you are hereby designated as the 3d Marine Division Special Security Officer.
2. You will become thoroughly familiar with the pertinent references in carrying out your assigned duties.
3. This appointment supersedes all previous appointments as 3d Marine Division Special Security Officer.

SIGNATURE

Copy to:

COMNAVINTCOM (NIC-44/OP-00904)

CMC (INTS)

CINCPACFLT (SSO)

CG, COMMARFORPAC (SSO)

CG, III MEF (SSO)

CO, Hq Bn (Scty Mgr)

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Commanding Officer, unit
To: Commanding General, 3d Marine Division (Security Manager)
Via: (As appropriate)

Subj: REPORT OF UNANNOUNCED AFTER HOURS SECURITY INSPECTION(S)
FOR THE MONTH OF

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K
(c) (Security Violation Report)

1. Per references (a) and (b), an unannounced after hours security inspection was conducted on (date) for all areas within (unit) where classified material is used and/or stored. The inspection was conducted to determine whether classified material is properly secured and all administrative requirements contained in the references are being complied with.

2. No discrepancies or security violations were noted during the inspection.

-or-

During the inspection, (describe what was discovered; immediate action taken by inspector(s); and what corrective action(s) were taken.

-or-

Details of the security violation discovered are contained in reference (c).

SIGNATURE

Figure 2-9. Unannounced After Hours Security Inspection Report
Format

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Commanding Officer, unit
To: Commanding General, 3d Marine Division (Security Manager)
Via: (As appropriate)

Subj: REPORT OF RANDOM ENTRANCE AND EXIT SECURITY INSPECTION(S)
FOR THE PERIOD ENDING

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K
(c) (Security Violation Report)

1. Per references (a) and (b), a Random Entrance and Exit Security Inspection was conducted on (date) for all personnel entering and exiting building(s) (bldg No's) wherein classified material is maintained/utilized.
2. No discrepancies or security violations were noted during the inspection.

-or-

During the inspection, (describe what was discovered; immediate action taken by inspector(s); and what corrective action(s) were taken.

-or-

Details of the security violation discovered are contained in reference (c).

SIGNATURE

SOP FOR IPSP

HEADING

5510
ID SYMBOL
(DATE)

From: Commanding Officer, unit
To: Commanding General, 3d Marine Division (Security Manager)
Via: (As appropriate)

Subj: REPORT OF INFORMATION SYSTEMS SECURITY INSPECTION(S)
FOR THE MONTH OF

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K
(c) (Security Violation Report)

1. Per references (a) and (b), an Information Systems Security Inspection was conducted on (date) for all areas within (unit), that utilize word processing, microcomputers, associated hardware and software.
2. No discrepancies or security violations were noted during the inspection.

-or-

During the inspection, (describe what was discovered; immediate action taken by the inspector(s); and what corrective action(s) were taken.

-or-

Details of the security violation discovered are contained in reference (c).

SIGNATURE

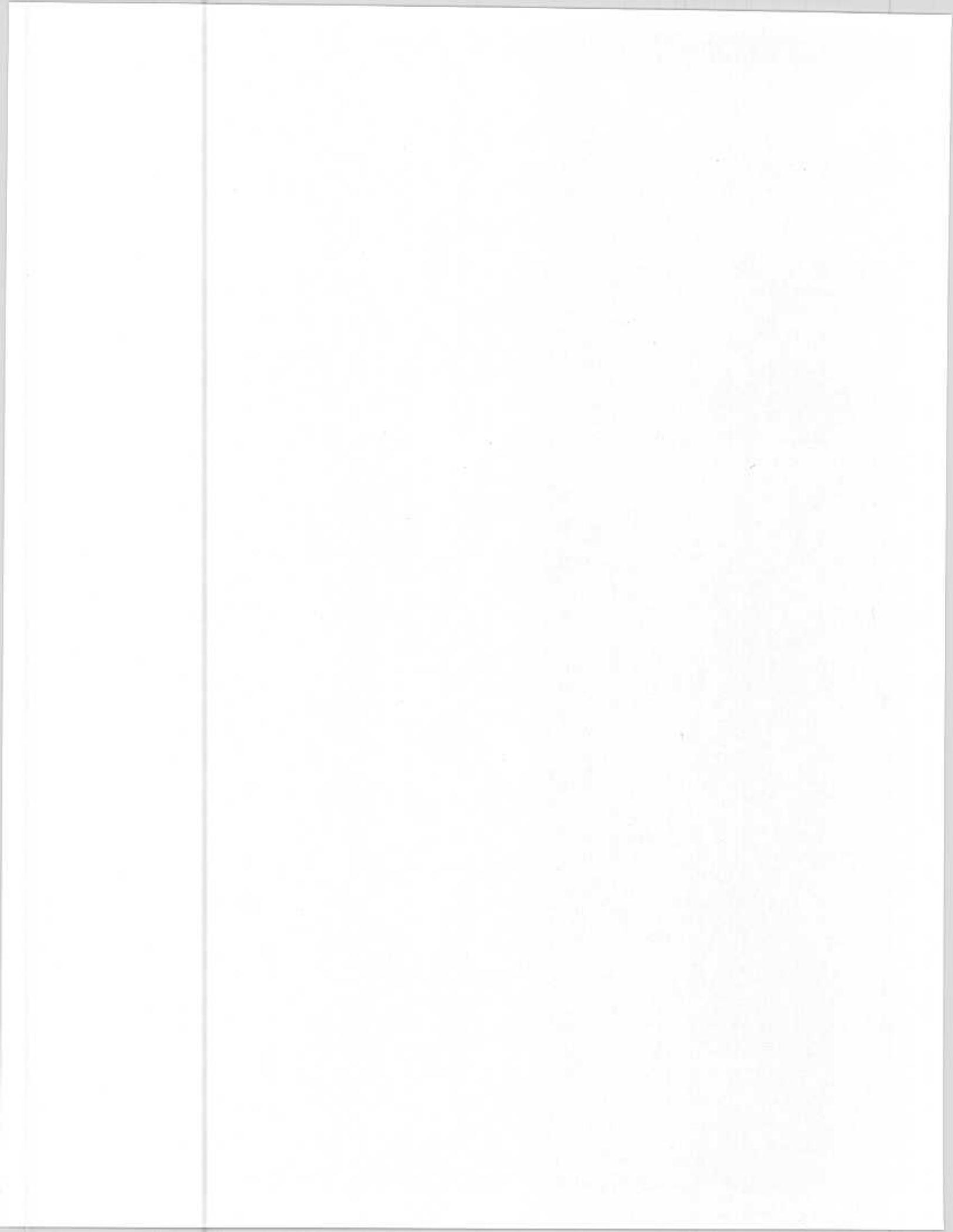
Figure 2-11. Information Systems Security Inspection Report
Format

SOP FOR IPSP
CHAPTER 3
SECURITY EDUCATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	3000	3-3
PURPOSE.....	3001	3-3
RESPONSIBILITY.....	3002	3-3
MINIMUM REQUIREMENTS.....	3003	3-3
DEBRIEFING.....	3004	3-6
CONTINUING SECURITY AWARENESS.....	3005	3-7

FIGURE

3-1 SECURITY TERMINATION STATEMENT.....	3-8
---	-----



SOP FOR IPSP

CHAPTER 3

SECURITY EDUCATION

3000. BASIC POLICY. Every unit within the 3d Marine Division shall establish and maintain an active security education program to instruct all personnel, regardless of their position, rank, or grade, in security policies and procedures. Specific guidance for the content of minimum briefing requirements are outlined in chapter 3 of reference (c) and this Order.

3001. PURPOSE

1. The purpose of a security education program is to make all personnel aware of the need to protect classified information from disclosure to unauthorized persons, not the least of which are those intelligence organizations employed by nations whose interests are hostile to those of the United States.

2. All personnel, whether they have been granted access to classified material, must understand and know specific safeguards to employ to protect information, classified or not, that could be used by forces hostile to U.S. interests. A primary goal of the security education program is the establishment of basic habits and discretion that result in automatic application of security measures.

3002. RESPONSIBILITY

1. The Commanding General, through the Division Security Manager, is responsible for the security education program of the 3d Marine Division. The Commanding Officer, Headquarters Battalion, is responsible for the conduct of the security education program and for maintaining adequate records of training conducted for all Headquarters Battalion personnel, including General and Special staff sections of the Division Headquarters.

2. All section heads and officers in charge, are responsible for identifying specific security education requirements for their own particular sections. All section heads and officers in charge are responsible for ensuring that adequate on-the-job training is conducted and recorded per reference (c) and this Order.

3. Subordinate unit commanding officers are responsible for the establishment, conduct and administration of their own unit security education program per reference (c) and this Order.

3003. MINIMUM REQUIREMENTS

1. Checkin. During the check-in process, unit commanders will ensure that all personnel are briefed on the following items of information. This briefing may be oral or written and will be recorded and records maintained for two years by unit security managers.

- a. Identity of unit security manager and assistant.
- b. Individual responsibility to protect classified information and material.
- c. Notification that the individual has not been granted access to classified information.
- d. Notification that the individual must attend the unit orientation briefing for all newly joined personnel regardless of rank or position to which assigned.

2. Indoctrination. Unit commanders will ensure that all newly joined personnel receive an indoctrination briefing explaining the Information Security Program within their unit and the 3d Marine Division. The indoctrination brief will be conducted in a classroom environment. The unit security manager will ensure that the instructor(s) is thoroughly trained and capable of answering any questions that may be asked during the presentation. The briefing for sergeants and below will include, as a minimum, items (a) through (l) listed below. The briefing for officers and staff noncommissioned officers will include, as a minimum, items (a) through (q) listed below. The Security Manager of Headquarters Battalion will ensure that members of the Division General and Special staff sections receive this briefing. This briefing will be recorded and records maintained for two years by unit security managers.

- a. Identify by name and position the unit security manager and assistant.
- b. The effects upon individuals of unauthorized disclosure of classified material to personnel not authorized to receive it.
- c. Personal behavior which could make an individual ineligible for a security clearance.
- d. Misconduct of others that should be reported to the section NCOIC, OIC or unit security manager.
- e. Individual responsibilities for the control of classified material in their possession.
- f. Requirement to verify another's clearance and access to classified material before disclosing subject information.
- g. Telephone security and the use of STU III telephones.
- h. Individual requirement to report contact with foreign nationals, attempts of solicitation for information, or attempts to obligate by blackmail.
- i. Requirement for all individuals with top secret clearance,

SCI access or access to special access programs to report all foreign travel in advance to the unit security manager. All travel to designated countries to be reported to the security manager by all personnel regardless of level of clearance held.

j. Security clearance eligibility and administrative procedures.

k. Security education (unit requirements, work section requirements, annual and bi-annual requirements).

l. Marking classified material.

m. Preparation and control of working papers.

n. Reproduction of classified material.

o. Host responsibilities at meetings where classified material will be discussed or distributed.

p. Proper transmission procedures for classified material.

q. Destruction of classified material.

3. Orientation/Access. On being granted access to classified information, all personnel will receive an orientation/access briefing, explaining their responsibilities for protecting the information with which they work.

4. On-the-job-training. Work section supervisors, including General and Special staff sections, will ensure that subordinates understand and practice security requirements that impact on activities within their work section. This training may be oral, written or a combination of both. This training will be recorded and records retained for two years by work section supervisors.

5. Annual Refresher. A refresher briefing will be given annually to all personnel with access to classified material and, if considered prudent, to those personnel without access. This briefing will cover those areas of information related to the security of classified information outlined in paragraph 3-4 of reference (c). This briefing will be recorded and records maintained for two years by unit security managers.

6. Foreign Travel. All personnel having a top secret clearance, SCI access or access to special access programs, must report all personal foreign travel in advance per paragraph 5-6 of reference (c). All travel to designated countries listed in Exhibit 5A of reference (c) must be reported by all personnel, without regard to security clearance level or access eligibilities. Unusual patterns of personal foreign travel by cleared personnel, or their failure to report such travel as required must be reported. Unit security managers can receive assistance concerning foreign travel

briefings from the Division Security Manager. Foreign travel briefings may be oral or written, or a combination of both. Foreign travel briefings for personnel with SCI access will be administered by the Division SSO. The SSO will maintain records of these briefings for two years. Unit security managers will administer foreign travel briefs for personnel with Top Secret clearances or for personnel that travel to those countries listed in Exhibit 5A of reference (c). These briefings will be recorded and records maintained for two years by unit security managers. Unit commanders will ensure that the requirement to report foreign travel is included in all orientation/access, annual refresher and counterespionage briefings.

7. Counterespionage Briefing. All personnel with access to classified information, secret or above, must receive a counterespionage briefing every two years. The briefing will be conducted by a member of the Naval Criminal Investigative Service. This briefing will be recorded and records maintained for two years by unit security managers.

8. NATO Briefing. All personnel who require access to NATO information must be briefed on NATO security procedures before access is granted. NATO security briefing requirements are outlined in OPNAVINST C5510.101. Unit commanders will ensure that personnel granted access to NATO information are made aware of the NATO specific debriefing requirements. This briefing and the attached debriefing will be maintained by unit security managers for two years from the date of the debrief.

9. Sensitive Compartmented Information (SCI). The Special Security Officer (SSO) is responsible for briefing those personnel who are to have access to SCI. This briefing will be recorded and records maintained in accordance with applicable directives by the administrative section of the SSO.

3004. DEBRIEFING

1. All 3d Marine Division personnel will be debriefed per chapter 3 of reference (c), special access program directives and this Order. Debriefs will be administered for the following reasons.

a. When a member of the command who had access to classified material is transferred (PCS/PCA).

b. Prior to termination of active military service or civilian employment, or temporary separation for a period of sixty days or more, including sabbaticals and leave without pay;

c. At the expiration of a limited access authorization;

d. When a security clearance is revoked for cause; or

- e. When a security clearance is administratively withdrawn.
 - f. When a member of the command inadvertently gains access to information which they are not eligible to receive.
2. Inadvertent disclosure (paragraph 1.f. above) when related to SCI material, will be handled and records prepared in accordance with applicable directives by the SSO.
 3. A Security Termination Statement (OPNAV Form 5511/14) figure 3-1, will not be executed when an individual is transferred (PCS/PCA).
 4. For those instances when a Security Termination Statement is executed (paragraph 1.b. through 1.f. above), the instructions contained in paragraph 3-12 of reference (c) will be followed for filing and/or forwarding the completed statement.

3005 CONTINUING SECURITY AWARENESS. To enhance security on a continuous basis, unit security managers will ensure that all personnel are frequently exposed to security reminders such as signs, posters and bulletin board notices. Security notes may even be added to a unit's Plan of the Day bulletin, if utilized.

SOP FOR IPSP

<p>SECURITY TERMINATION STATEMENT OPNAV INST 5010.1001 DA FORM 45-888-1171</p>	<p><i>(Over name and address of appropriate Head of Service Corps primary command installation.)</i></p>
<p><u>Chief of Naval Operations</u></p>	
<p><u>(Op-09XXX)</u></p>	
<p><u>Washington, DC 20350</u></p>	
<p>1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (COM-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.</p>	
<p>2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.</p>	
<p>3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representatives on such matter prior to disclosing information which is or may be classified.</p>	
<p>4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to obtain classified information.</p>	
<p>5. I, <u>JAMES KEENE BRENELL</u>, have been informed and am aware that Title 18 U.S.C. Sections 793-795, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand paragraph F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the provisions of law relating to such class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders the subject liable therefor, as provided by Title 18 U.S.C. 1001.</p>	
<p>6. I have/has not received an oral debriefing.</p>	
<p>SIGNATURE OF WITNESS</p>	<p>SIGNATURE OF EMPLOYEE OF MEMBER OF NAVAL OR MARINE CORPS SERVICE (To be filled in only by active duty personnel.)</p>
<p><i>Barbara Szvanski</i> TYPE PRINT NAME OF WITNESS Barbara Szvanski</p>	<p><i>James Keene Brenell</i> BY (Date)</p>
<p>0-14201</p>	

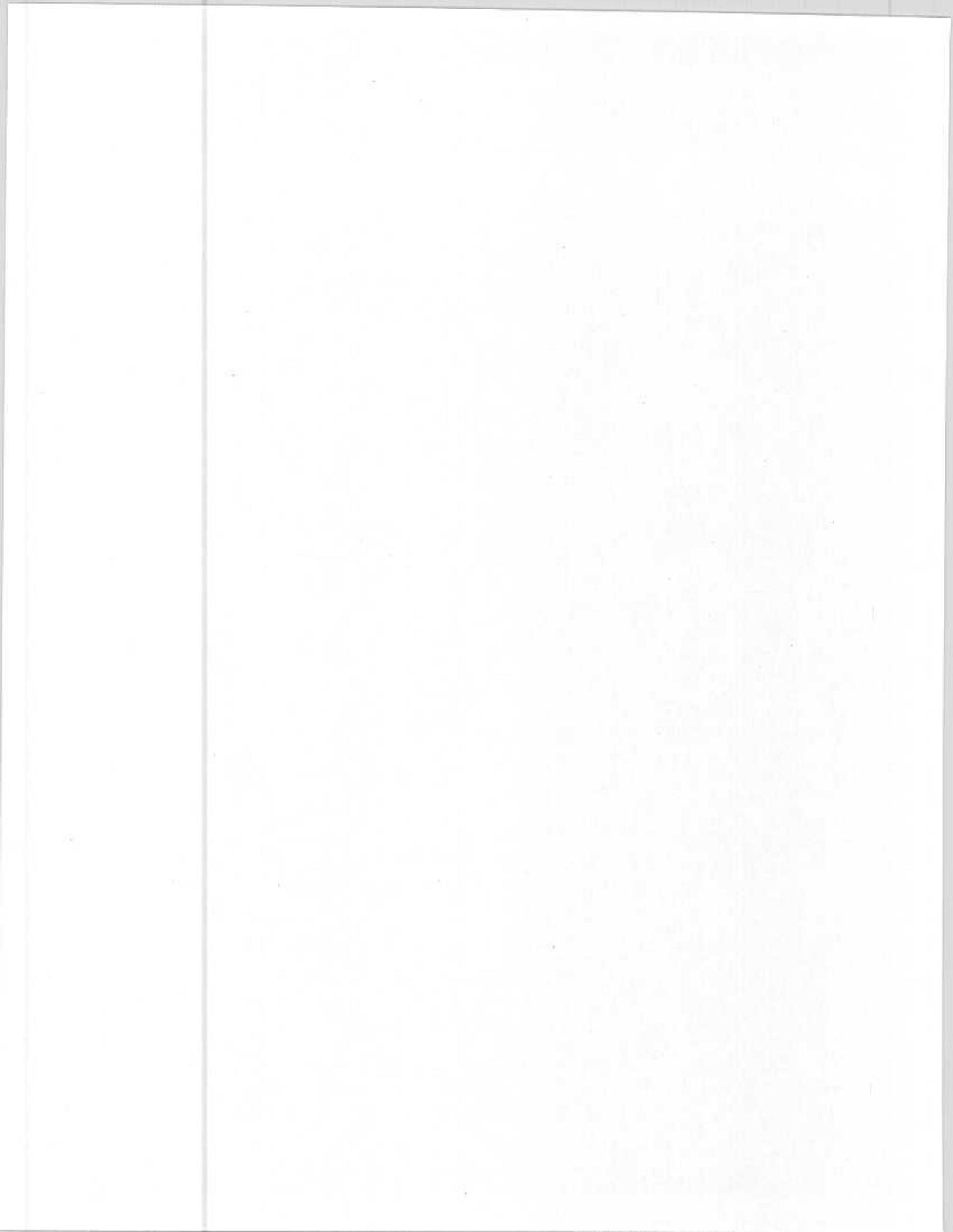
Figure 3-1. Security Termination Statement

SOP FOR IPSP

CHAPTER 4

COMPROMISE AND OTHER SECURITY VIOLATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	4000	4-3
COMPROMISE.....	4001	4-3
VIOLATIONS.....	4002	4-3
DISCOVERY OF LOSS, COMPROMISE OR POSSIBLE COMPROMISE.....	4003	4-4
PRELIMINARY INQUIRY.....	4004	4-4
INVESTIGATIONS.....	4005	4-4
INVESTIGATIVE ASSISTANCE.....	4006	4-4
REPORT OF FINDING CLASSIFIED MATERIAL PREVIOUSLY REPORTED AS LOST.....	4007	4-5
COMMUNICATIONS SECURITY MATERIAL SYSTEMS (CMS) INSECURITIES.....	4008	4-5
OTHER SECURITY VIOLATIONS.....	4009	4-5
REPORTING SECURITY VIOLATIONS.....	4010	4-5
IMPROPER TRANSMISSION.....	4011	4-6
RECORDS.....	4012	4-6
FIGURE		
4-1 SECURITY DISCREPANCY NOTICE.....		4-7



SOP FOR IPSP

CHAPTER 4

COMPROMISE AND OTHER SECURITY VIOLATIONS

4000. BASIC POLICY. There are two types of security violations. One results in the loss, compromise or possible compromise of classified information. The other involves a failure to adhere to security regulations but does not result in a loss, compromise, or possible compromise. The loss, compromise or possible compromise of classified information presents a threat to national security. The seriousness of that threat must be determined and measures taken to negate or minimize the adverse effect of the compromise. Chapter 4 of reference (c) contains explicit and detailed guidance concerning action to be taken in the event of loss, compromise, possible compromise or other security violations.

4001. COMPROMISE. Compromise is the disclosure of classified information to a person who is not authorized access. The unauthorized disclosure may have occurred knowingly, willfully or through negligence. Military personnel are subject to disciplinary action, either in federal courts or under the Uniform Code of Military Justice (UCMJ), as well as administrative sanctions, if they disclose classified information to an unauthorized person or violate any provisions of this Order and other pertinent regulations governing the protection of classified information.

4002. VIOLATIONS

1. A violation occurs when security regulations and/or procedures are violated. All individuals who become aware of a security violation(s) will report it to the unit security manager immediately. The security manager will direct the necessary action to preclude recurrence.
2. Obviously, violations involving the compromise of classified information are of greater concern since they present a significant threat to national security. However, other security violations must also be treated seriously, since they may indicate a weakness in a command's security program. For this reason, security violations of either type must be vigorously investigated and prevented from recurring by correcting the problems causing the violation.
3. Security violations reflect negatively on an individual's eligibility for clearance and access to classified information. Repeated security violations can be cause for denial or revocation of the individual's clearance, even when the violations are not separately punishable. Clearance and access to classified information are granted only if "clearly" consistent with the interest of national security. Repeated security violations do not meet this criteria.

4003. DISCOVERY OF SECURITY VIOLATIONS

1. Any individual in the 3d Marine Division who becomes aware of a security violation will:

a. Notify their unit commander or security manager immediately. For security violations discovered in General or Special staff sections of the Division Headquarters, the Division Security Manager will be notified.

b. The commanding officer/security manager will determine if there is any indication of compromise or potential for compromise, i.e., classified material, improperly secured/security containers left open, the individual(s) identified as responsible for the security container will be recalled and conduct a complete inventory of all the classified material in the container.

2. When classified material has been reported as lost, compromised or subject to compromise, the responsible command will:

a. Regain, or attempt to regain, custody of the classified information, when possible.

b. If recovery of the information is not possible, attempt to identify the location or possible location of the material. Any information identifying the location of classified material not under U.S. control will be classified at the same level as the unretrieved material.

c. The command with custodial responsibility will be notified immediately in accordance with the guidance provided in chapter 4 of reference (c).

4004. PRELIMINARY INQUIRY. Preliminary inquiries will be initiated and conducted in accordance with the detailed guidance provided in paragraph 4-4 of reference (c). The preliminary inquiry will be completed within 72 hours of initiation. Whenever a preliminary inquiry is initiated, the Division Security Manager will be notified immediately by phone.

4005. INVESTIGATIONS. When the circumstances surrounding a security violation warrant, or when the next senior command directs, a JAG Manual investigation will be conducted to answer, in detail, the incident. All JAG Manual investigations will be conducted per the current edition of reference (t) and chapter 4 of reference (c).

4006. INVESTIGATIVE ASSISTANCE. Successful completion of an investigation may, under certain circumstances, require professional or technical assistance.

1. Commanding officers may ask the Naval Criminal Investigative

Service (NCIS) field office for investigative assistance in cases where their commands lack either the resources or the capabilities to conduct specific investigations. Such requests may be made at any time during the course of an investigation, regardless of whether NCIS initially declined investigative action. The Division Security Manager will be advised by phone of any requests for investigative assistance from NCIS.

2. Investigative assistance may be requested from the III MEF Staff Counterintelligence Officer via the Division Security Manager.

4007. REPORT OF FINDING CLASSIFIED MATERIAL PREVIOUSLY REPORTED AS LOST. Per reference (c), when classified material previously reported as lost is subsequently found under circumstances which conclusively preclude its having been subjected to compromise, this fact will be reported to all who were notified of the loss. These reports, if destined for organizations or originators outside the 3d Marine Division, will be prepared and submitted to the Division Security Manager for review and release.

4008. COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS) INSECURITIES. CMS insecurities will be acted on by the CMS custodian per reference (m) and other pertinent CMS directives. The CMS custodian will keep the security manager informed and route all correspondence pertaining to insecurities via the security manager for concurrence.

4009. OTHER SECURITY VIOLATIONS. Other security violations which involve a failure to adhere to security regulations, but does not result in a loss, compromise or possible compromise are subject to serious investigation by the command making the discovery.

1. Unit security managers will vigorously investigate these types of security violations and take the appropriate action to ensure that they do not recur.

2. Unit security managers are not required to report these types of investigations to the Division Security Manager. Unit security managers are encouraged to report these types of violations to the Division Security Manager by phone. The intent of the reporting would be to identify trends or potential problems that could be passed to other units of the Division.

4010. REPORTING SECURITY VIOLATION. All security violations will be investigated and reported in accordance with the detailed guidance (including examples) provided in chapter 4 of reference (c). All reports destined for organizations or originators outside the 3d Marine Division, will be prepared and submitted to the Division Security Manager for review and release.

4011. IMPROPER TRANSMISSION

1. Within the 3d Marine Division, if a unit/section receives classified material that has been improperly mailed, shipped, addressed, packaged, handled or transmitted, that unit/section will immediately deliver the material and envelope/container to the unit security manager. For General and Special staff sections of the Division Headquarters, such material will be delivered to the Division Security Manager. The security manager of the receiving unit will determine whether the material has been subjected to compromise. When circumstances indicate the classified material has been subjected to compromise, the receiving command is to immediately notify the sending command. For the Division, material to be considered as having been subjected to compromise is material that has been handled by a foreign postal system, its shipping container has been damaged in shipment to the extent that it's contents are exposed or it has been transmitted over unprotected circuits (e.g. facsimile, telephone, teletype, data links, etc.). Material that has been subjected to loss of control is material that was mailed via the U.S. postal system and not registered. When circumstances indicate that information was not subjected to compromise or loss of control, the unit/Division CMCCO will prepare and forward to the sending command a Security Discrepancy Notice (OPNAV 5511/51) shown in figure 4-1.

2. If a command is notified that classified material has been subjected to compromise due to improper transmission, the sending command is to initiate a Preliminary Inquiry into the loss, compromise or possible compromise. If a command is notified by OPNAV 5511/51 of an improper transmission security violation not involving a possible compromise, the command transmitting the material should investigate the violation and take corrective action to prevent its recurrence.

4012. RECORDS. All records/reports associated with a security violation will be maintained by the unit security manager for two years and then destroyed.

SOP FOR IPSP

SECURITY DISCREPANCY NOTICE		
OPNAV 511.1/1 (5-40) 574 0101-015-0311 (This form replaces OPNAV 511.1/1, 22 and 24 which are obsolete)		
FROM	DATE	
(Insert 09, 88)		
U. S. OPNAVINST 5510.3 SERIES		
ENCL		
TO: (Note - This form may be mailed in a window envelope.)		
1. Reference (a) has been found to be inconsistent with or in contradiction of reference (a) for the reason(s) checked below. 2. If applicable, corrective action should be taken and where this involves changing classification, all holders of reference (a) should be notified accordingly.		
IMPROPER TRANSMITTAL/PACKAGING		
SENT VIA NON-REGISTERED/ NON-CERTIFIED MAIL	CLASSIFICATION NOT MARKED ON INNER CONTAINER	RECEIVED IN POOR CONDITION; COMPROMISE IMPROBABLE
SENT IN SINGLE CONTAINER	NO RETURN RECEIPT	ADDRESSED IMPROPERLY
MARKINGS ON OUTER CONTAINER DIVULGE CLASSIF. OF CONTENTS	INADEQUATE WRAPPING; NOT SECURELY WRAPPED OR PROTECTED	OTHER (Specify)
CLASSIFICATION		
BASIC CLASSIFICATION QUESTIONABLE	DOCUMENT SUBJECT MARKING	CHART, MAP OR DRAWING MARKING
OVERALL MARKINGS	DOCUMENT MARKING	PHOTO, FILM OR RECORDING MARKING
PARAGRAPH/COMPONENT MARKINGS	MISCLASSIFICATION	OTHER (Specify)
CLASSIFICATION AUTHORITY		
CLASSIFICATION AUTHORITY IDENTIFIED OR UNAUTHORIZED	CLASSIFICATION MARKING DATA INCORRECT	DECLASSIFICATION (OR REVIEW) DATA OMITTED OR INCORRECT
OTHER (Specify)		
Fold here with face of form to show		
COMMENTS (Continue on reverse, if necessary)		
COPY TO: OP-CDD (WITH ADDRESSEE DELETED)		
SIGNATURE	TITLE	

Figure 4-1. Security Discrepancy Notice

SOP FOR IPSP

CHAPTER 5

COUNTERINTELLIGENCE MATTERS TO BE REPORTED

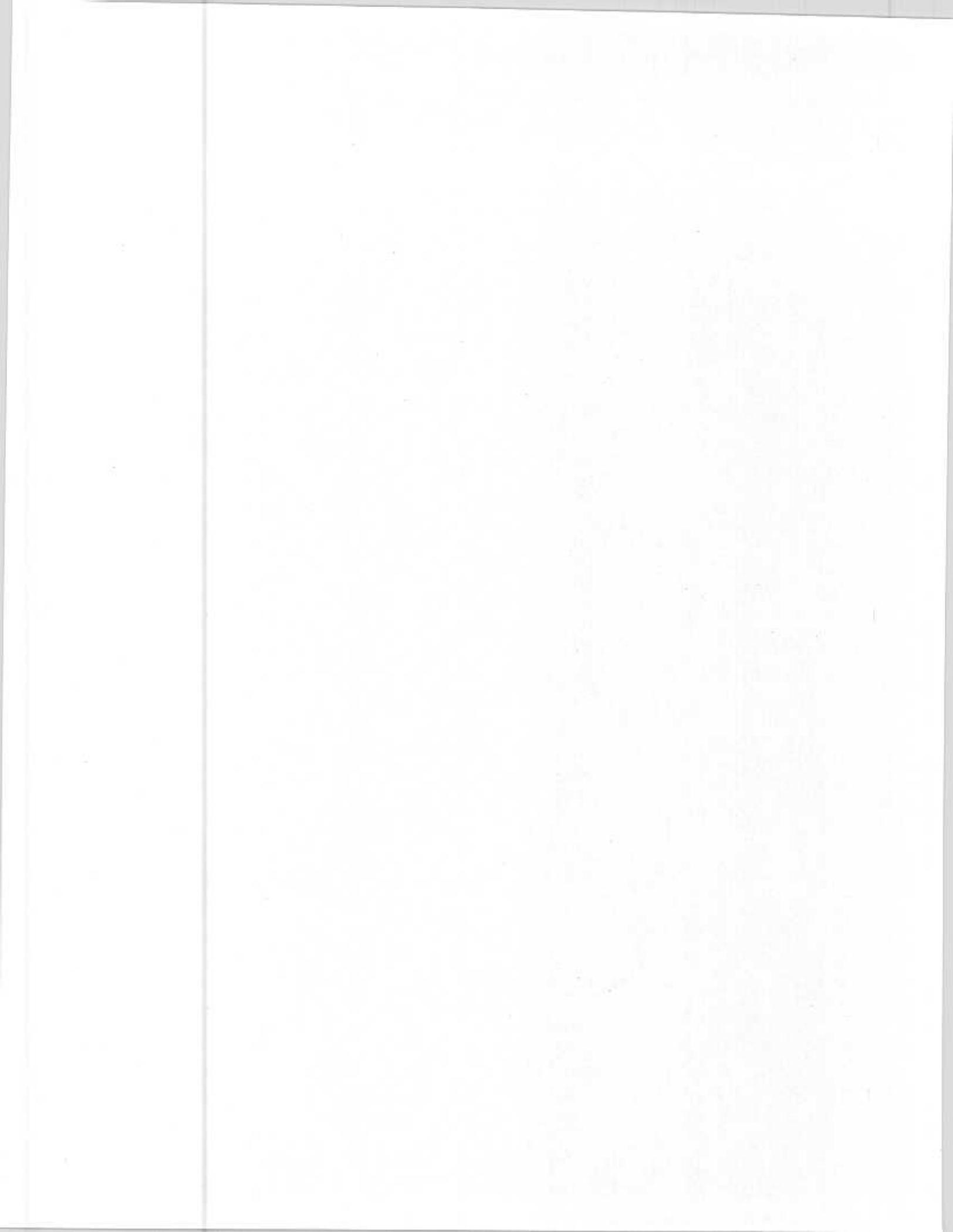
	<u>PARAGRAPH</u>	<u>PAGE</u>
COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO THE NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS)	5000	5-3

SOP FOR IPSP

CHAPTER 5

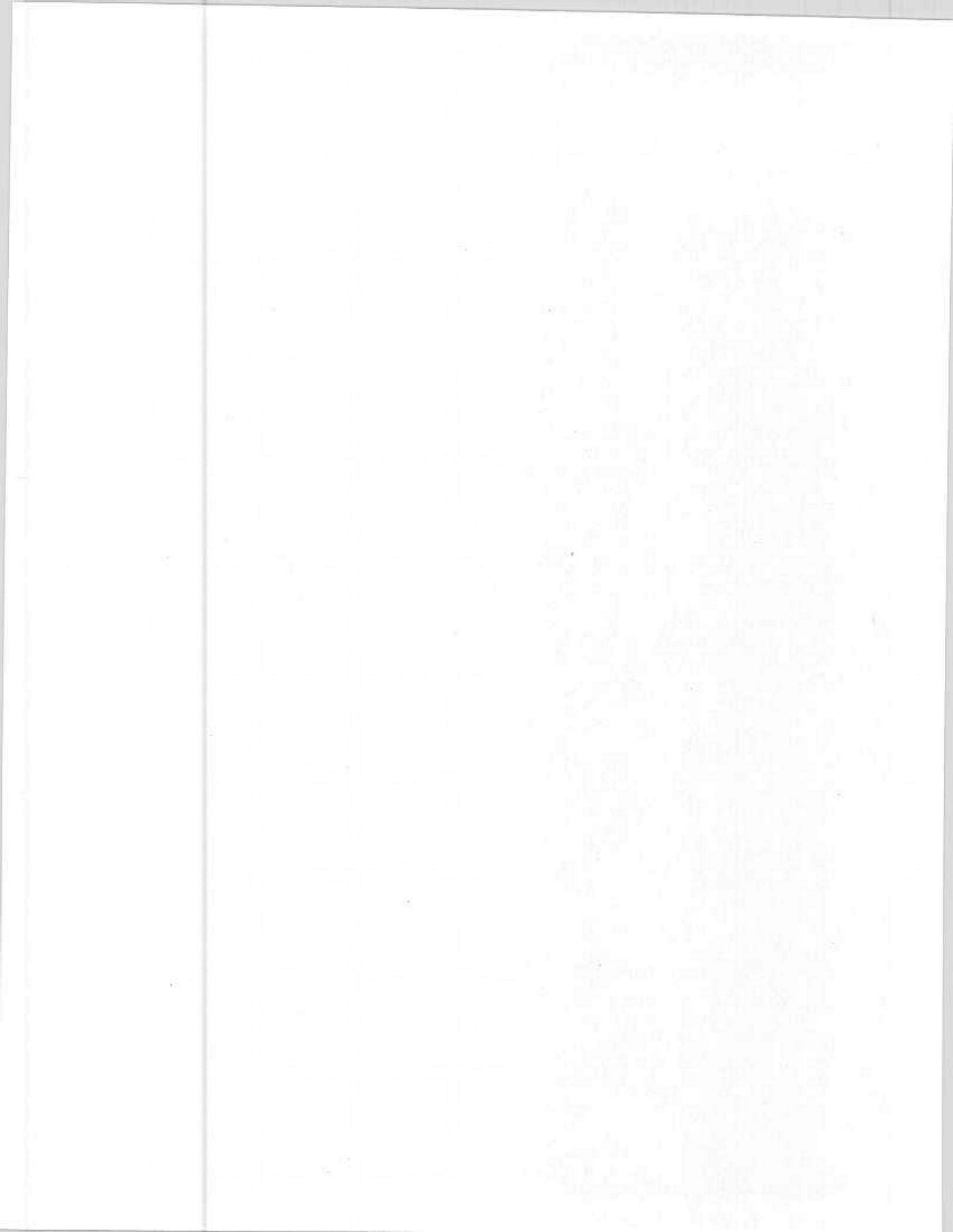
5000. COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO THE NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS). All personnel, whether or not they have access to classified information, will report any knowledge or information concerning the activities listed below. Such incidents must be reported to the commanding officer via the unit security manager. Certain matters affecting national security must be reported to the NCIS and/or other agencies for action per chapter 5 of reference (c). Unit security managers will make the determination and notification concerning NCIS or other agencies. The Division Security Manager will be notified immediately of reports of this nature by subordinate unit security managers.

1. Potential or actual acts of sabotage, espionage, deliberate compromise of classified information, or subversive activities. This includes any requests, other than through official channels, for classified information; or for unclassified information from any individual believed to be in contact with a foreign intelligence service.
2. Any form of contact, intentional or otherwise, with a citizen of a communist controlled country or a country currently hostile to the government of the U.S., see Exhibit 5A-1 of reference (c).
3. Any security violation in which a Preliminary Inquiry or a JAG Manual investigation is initiated.
4. Suicide or attempted suicide of any individual with access to classified information.
5. The unauthorized absence of any individual with access to classified information.
6. All personnel possessing a security clearance are required to report all personal foreign travel, in advance of the travel being performed, to their unit security manager.



SOP FOR IPSP
CHAPTER 6
CLASSIFICATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
ORIGINAL CLASSIFICATION AUTHORITY.....	6000	6-3
DERIVATIVE CLASSIFICATION AUTHORITY.....	6001	6-3
TENTATIVE CLASSIFICATION.....	6002	6-3
RECORDS.....	6003	6-4



SOP FOR IPSP

CHAPTER 6

CLASSIFICATION

6000. ORIGINAL CLASSIFICATION AUTHORITY

1. The Commanding General, Assistant Division Commander and the Chief of Staff are the only individuals within the Division who have Original Classification Authority (OCA). This authority is limited to secret and confidential and can not be delegated.
2. All recommendations for original classification from General and Special staff sections and subordinate unit commanders, will be submitted to the Commanding General via the Division Security Manager and Chief of Staff. Recommendations will contain detailed justification for the classification action per chapter 6 of reference (c).

6001. DERIVATIVE CLASSIFICATION AUTHORITY

1. Derivative classification is accomplished by the individual preparing the document when the individual incorporates, paraphrases, restates, or generates in new form information or material which is already classified.
2. The originating individual is accountable for the propriety of the classification assigned to the document. Individuals with "By Direction" authority or message release authority must ensure that classification markings are accurate and per chapter 9, paragraphs 9-2 through 9-11 of reference (c).
3. A derivative classifier must:
 - a. Respect the original classification decisions.
 - b. Verify the current level of classification insofar as practical.
 - c. Carry forward to any newly created document previously assigned dates or events for declassification, or a notation that the information cannot be automatically declassified without approval of the originating agency.

6002. TENTATIVE CLASSIFICATION. Per chapter 6 of reference (c), anyone who does not have OCA who originates information he/she believes should be classified, will proceed as follows:

- a. The information will be safeguarded as required for the intended classification.
- b. The information and cover sheet will be marked with the intended classification preceded by the word "Tentative".

c. The information will be forwarded, through the chain of command, via the security manager, to the next senior with OCA. Included in the body of the transmittal will be a statement to the effect that the information is tentatively marked to protect it in transit. A detailed statement justifying the tentative classification must accompany the document.

6003. RECORDS

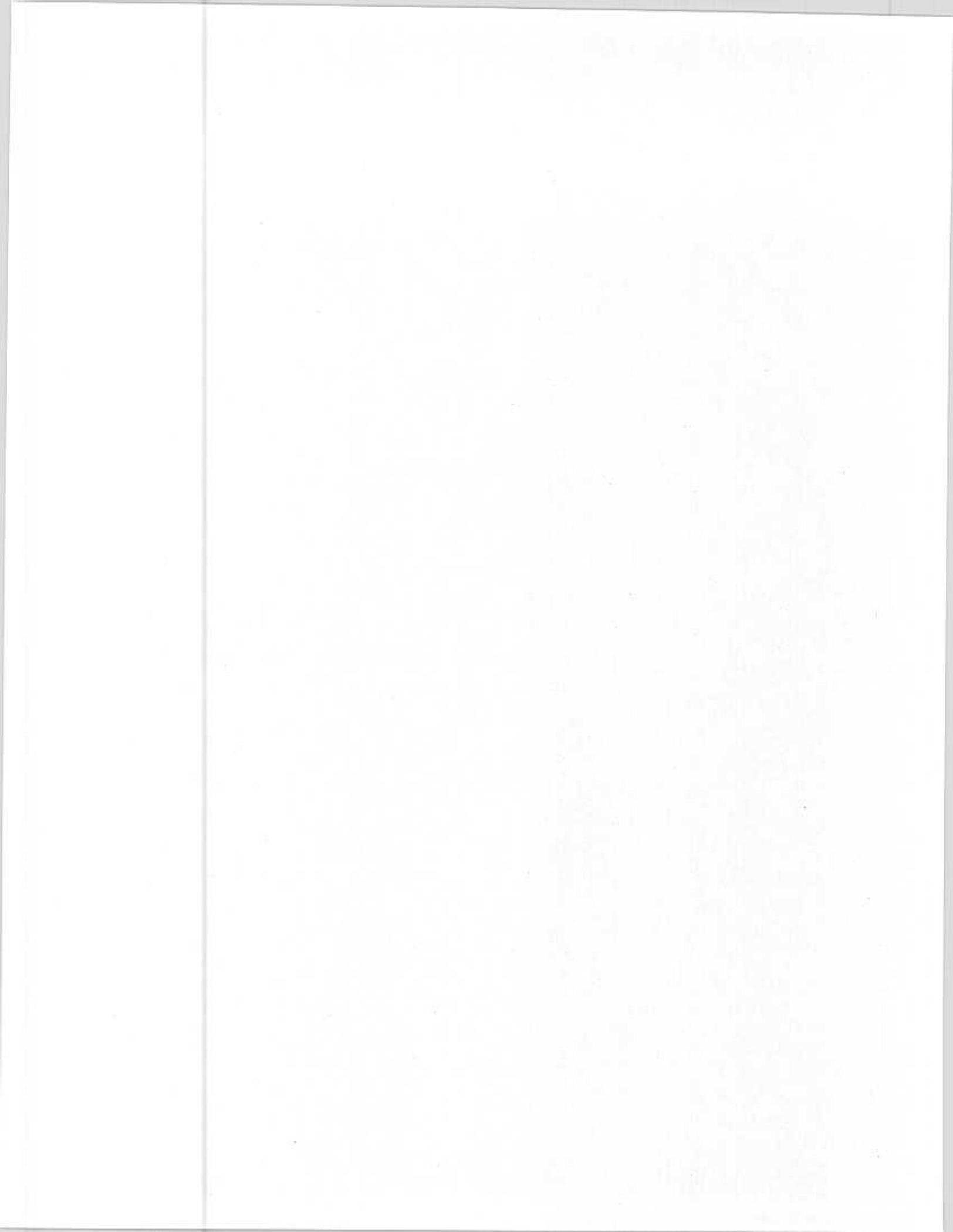
1. Original Classification. All records related to a recommendation for original classification will be submitted with the material per the instructions contained in chapter 6 of reference (c) and paragraph 6000 of this Order. After the OCA has reviewed the recommendation, all material will be sent to the Division CMCC for recording and retention. If the recommendation for original classification is approved, a copy of the product will be included with the recommendation package for record purposes. Records and material related to an original classification recommendation will be maintained for three years.
2. Derivative Classification. All records related to a document classified by derivative classification will be maintained by the unit/Division CMCC for three years. Derivative classification records will contain at a minimum the information listed below. A list of the derivative classification source documents will be attached to the file copy of the document.
 - a. Classification authority of source document(s).
 - b. Title of source document(s).
 - c. Classification of source document(s).
 - d. Declassification instructions of source document(s).

SOP FOR IPSP

CHAPTER 7

CLASSIFICATION GUIDES

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	7000	7-3
MAJOR SUBJECT CATEGORY GUIDES.....	7001	7-3
SECURITY CLASSIFICATION PRINCIPALS.....	7002	7-4



SOP FOR IPSP

CHAPTER 7

CLASSIFICATION GUIDES

7000. BASIC POLICY

1. Classification guides are prepared by Original Classification Authorities (OCA) for each system, plan, program or project involving classified information. Classification guides are promulgated to assist preparers of classified material in the proper implementation of the Classification Management Program.

2. The OPSEC Officer, in coordination with the unit/Division OPSEC Working Group, is responsible for preparation and assignment of classification guides for OPLANS, OPOORDERS, LOIs, SOPs and other documents related to unit/Division operations. OPNAVINST 5513 series promulgates classification guides and OPNAVNOTE 5510 series, provides an Index of Classification Guides. All members of the Division, and General and Special staff sections, will make maximum use of classification guides when preparing classified material. All questions concerning classification guides should be directed to the unit/Division OPSEC Officer or Security Manager.

7001. MAJOR SUBJECT CATEGORY GUIDES. Uniformly formatted classification guides are issued in the following subject categories:

a. OPNAVINST 5513.1; Specific Responsibilities for Preparation, Updating, Administrative Use and Detailed Index.

b. OPNAVINST C5513.2; Air Warfare Programs.

c. OPNAVINST S5513.2; Surface Warfare Programs.

d. OPNAVINST S5513.3; General Intelligence, Cover and Deception, and Investigative Programs.

e. OPNAVINST S5513.5; Undersea Warfare Programs.

f. OPNAVINST S5513.6; Communication and Satellite Programs.

g. OPNAVINST C5513.7; Mine Warfare Programs.

h. OPNAVINST S5513.8; Electronic Warfare Programs.

i. OPNAVINST S5513.9; Nuclear Warfare Programs.

j. OPNAVINST C5513.10; Miscellaneous Programs.

k. OPNAVINST 5513.11; Ground Combat Systems.

l. OPNAVINST S5513.12; Intelligence Research Projects.

- m. OPNAVINST S5513.13; Non-Acoustic Anti-Submarine Warfare.

7002. SECURITY CLASSIFICATION PRINCIPLES

1. Classification Criteria. Reference (c) states that unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt concerning the need to classify information, it should be safeguarded as if it were "Tentative Confidential" pending determination by the Division's OCA.

2. The material will be prepared and forwarded for a determination per the instructions contained in paragraph 6002 of this Order. When a classification determination has been made, proper markings shall be applied as required by reference (c).

3. A determination to originally classify shall be made by the OCA, only when the information meets one or more of the criteria listed below, and only when the disclosure of the information could reasonably be expected to cause a degree of damage to national security.

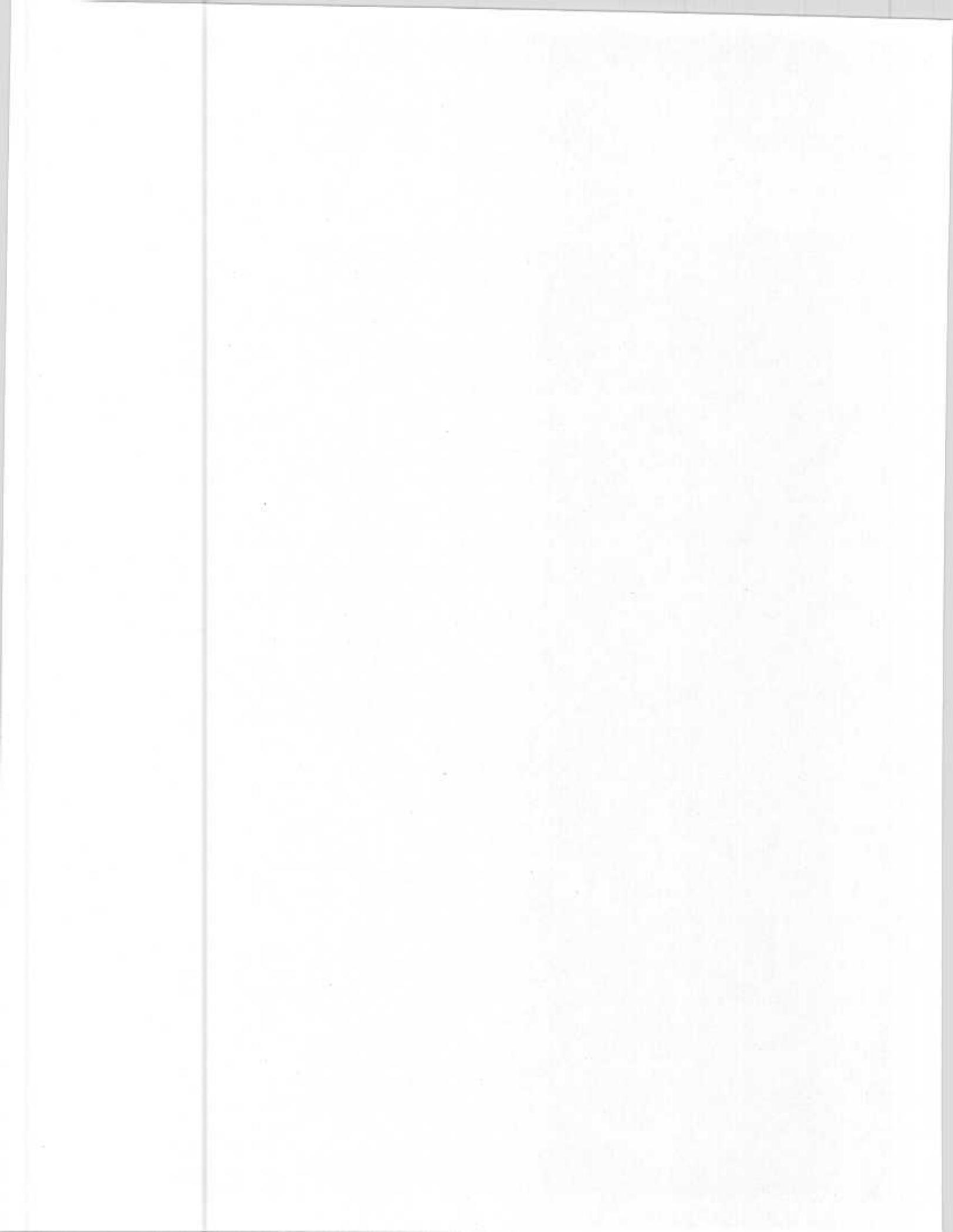
- a. Military plans, weapons or operations.
- b. Foreign government information.
- c. Intelligence activities, sources or methods.
- d. Foreign relations or foreign activities of the U.S..
- e. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.
- f. Cryptology.
- g. Confidential sources.
- h. Scientific, technological, or economic matters relating to national security.
- i. U. S. Government programs for safeguarding nuclear materials or facilities.

SOP FOR IPSP

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

	<u>PARAGRAPH</u>	<u>PAGE</u>
AUTHORITY.....	8000	8-3
ADMINISTRATIVE ACTION.....	8001	8-3
ANNUAL REVIEW/INVENTORY.....	8002	8-3
ADDITIONAL INVENTORIES.....	8003	8-4
FIGURE		
8-1 ANNUAL REVIEW/INVENTORY BOARD MEMBER APPOINTMENT LETTER.....		8-5



SOP FOR IPSP

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

8000. **AUTHORITY.** The Commanding General, Deputy Division Commander and the Chief of Staff are the only individuals authorized to make decisions concerning declassification, downgrading and upgrading information classified per reference (c). This authority is limited to information which they have classified as OCAs. Recommendations for downgrading, declassification or upgrading action will be submitted to the Commanding General via the Division Security Manager and the Chief of Staff.

8001. **ADMINISTRATIVE ACTION.** The authority to downgrade or declassify is not to be confused with administrative responsibility of a holder of classified information to downgrade or declassify as directed by classification instructions, the continued protection guidelines or the instructions on the document. The authority is also not to be confused with a derivative classifier's responsibility to carry forward downgrading and declassification markings of a source document per reference (c).

8002. **ANNUAL REVIEW/INVENTORY.** Per paragraph 8-4 of reference (c), Navy and Marine Corps commands are no longer required to conduct a systematic review for declassification.

1. The Division Security Manager will direct an annual review/inventory of all classified holdings at the General and Special staff level. Subordinate unit security managers will also direct an annual review/inventory of classified holdings. The review/inventory will be convened no later than 15 February of each year.

2. The purpose of Annual Review/Inventory Boards convened by units of the 3d Marine Division will be to reduce classified holdings to the minimum amount consistent with the mission of the command and ensure accurate accounting of classified holdings.

3. Members of the Division Annual Review/Inventory Board will normally consist of the personnel listed below. Figure 8-1 is a sample letter for appointment to the Annual Review/Inventory Board.

a. At the Division Headquarters:

- (1) CMCC Officer (recorder)
- (2) AC/S, G-1 (senior member)

- (3) AC/S, G-2
- (4) AC/S, G-3
- (5) AC/S, G-4
- (6) AC/S, G-6

b. Subordinate units:

- (1) CMCC Officer (recorder)
- (2) S-1
- (3) S-2
- (4) S-3
- (5) S-4
- (6) S-6

8003. ADDITIONAL INVENTORIES. In addition to the Annual Review/Inventory Board, an inventory of all classified holdings will be accomplished under the following circumstances:

1. Quarterly CMCC Officers will inventory classified holdings of all subordinate SCPs.
2. Upon change of custodian(s) for a CMCC, SCP, or SCCP. This inventory will be completed at least 10 days prior to the old custodian's departure or reassignment in order to resolve discrepancies.
3. When any security container or storage area is found unsecured and unattended.
4. When directed by special instructions or the unit security manager.

SOP FOR IPSP

HEADING

5511
ID SYMBOL
(DATE)

From: Commanding General/Commanding Officer
To: (List Board Members)

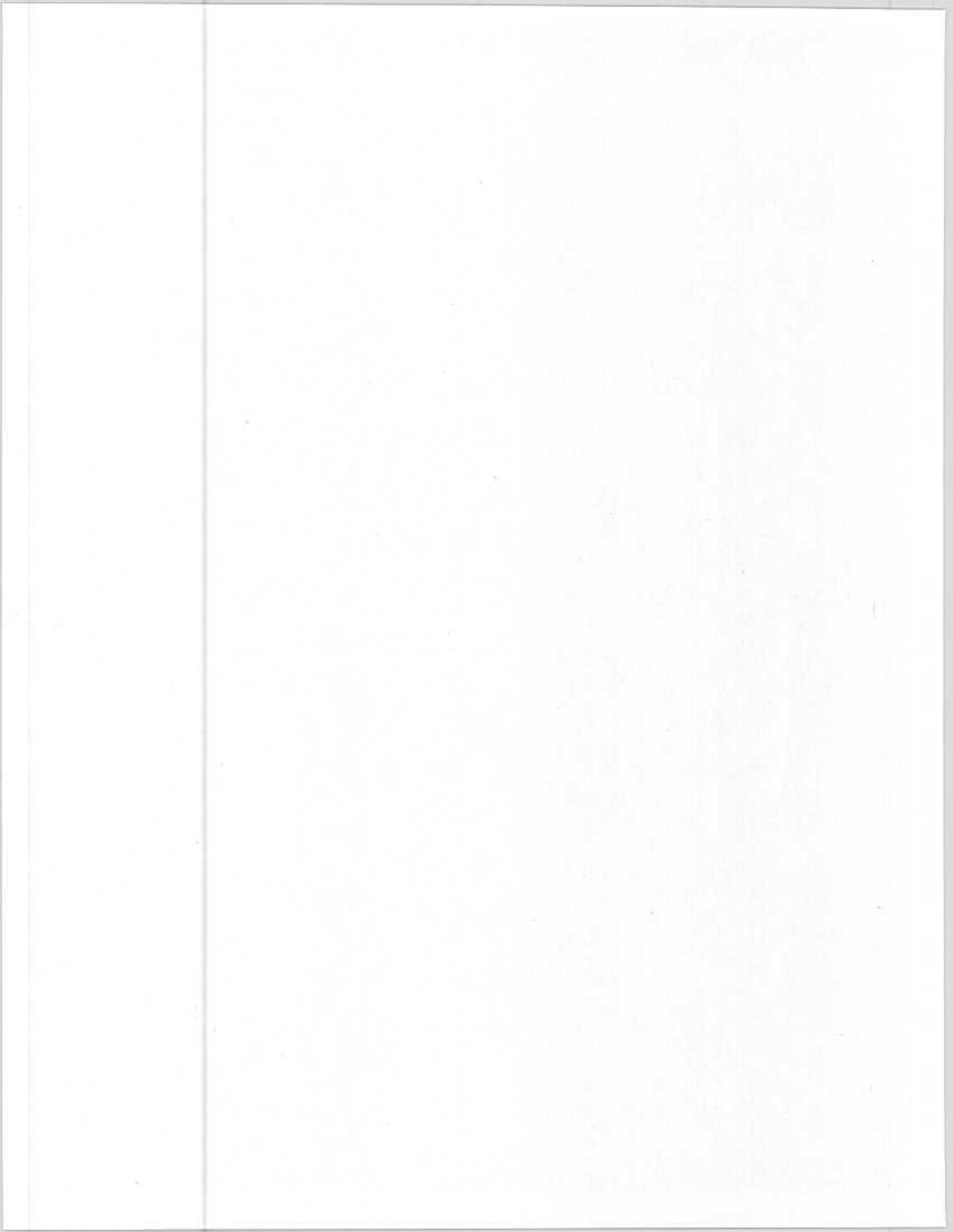
Subj: APPOINTMENT OF MEMBERS FOR THE ANNUAL REVIEW/INVENTORY
BOARD

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. Per the references, you are hereby assigned to the Annual Review/Inventory Board.
2. The purpose of this Board is to review and inventory all classified documents held by the (unit) CMCC, and to determine which documents should be retained, downgraded, or destroyed per the references.
3. Board members must possess at least a (level of clearance and access) to participate.
4. All Secondary Control Points will review their classified holdings prior to the Board being held, and submit their written results to the (unit) CMCC on or prior to the day of the Board.
5. The Senior Member will report the results of the actions taken by the Board to the Commanding General/Commanding Officer (Security Manager) in writing.

SIGNATURE

Figure 8-1. Annual Review/Inventory Board Member Appointment Letter



SOP FOR IPSP

CHAPTER 9

MARKING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	9000	9-3
ADDITIONAL GUIDANCE.....	9001	9-3
DEFINITION.....	9002	9-3
DRAFTER RESPONSIBILITIES.....	9003	9-3
APPROVING AUTHORITY RESPONSIBILITIES.....	9004	9-3
RECORDS REQUIRED.....	9005	9-3
MARKING OTHER CLASSIFIED MATERIAL.....	9006	9-4
SPECIAL ACCESS PROGRAM MATERIAL.....	9007	9-6

FIGURE

9-1	SAMPLE PROPERLY MARKED CLASSIFIED MESSAGE.....	9-7
9-2	SAMPLE FORMAT LISTING SOURCE DOCUMENTS.	9-8
9-3	SAMPLE PROPERLY MARKED CLASSIFIED DOCUMENT.....	9-9
9-4	SAMPLE PROPERLY MARKED CLASSIFIED DOCUMENT.....	9-10
9-5	SAMPLE TRANSMITTAL/COVER LETTER.....	9-11
9-6	SAMPLES COLOR CODED CLASSIFICATION LABELS.....	9-12

SOP FOR IPSP

CHAPTER 9

MARKING

9000. BASIC POLICY. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading and declassification actions. Therefore, all classified materials will be marked in a manner that leaves no doubt as to the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material. Chapter 9 of reference (c) provides detailed guidance (with examples) for marking classified material, including exceptions to basic marking requirements.

9001. ADDITIONAL GUIDANCE. Additional guidance may be found in Chapter II of the current edition of SECNAVINST 5216.5, Department of the Navy Correspondence Manual and Volume V, Joint Operations Planning System.

9002. DEFINITION. Per reference (c), classified material is any product embodying classified information.

9003. DRAFTER RESPONSIBILITIES. The drafter of classified material is responsible to ensure that classified markings are accurately carried forward from source document(s) to the newly created material. Attention to this requirement must start with the initial draft.

9004. APPROVING AUTHORITY RESPONSIBILITIES. Heads of General and Special staff sections or individuals with "By Direction" authority and any individual who approves the creation of classified material is personally responsible for ensuring that classification markings are correctly applied and that adequate records to support the classification markings are maintained.

9005. RECORDS REQUIRED. Records will be maintained by each section which creates classified material. The classification record will be apart of or attached to the file copy of the material.

1. Messages. Per reference (c), a "Classified by" line is not required on messages. The originator of the message is considered the responsible classifier and must maintain records to identify the source. A sample of a properly marked classified message is shown at figure 9-1.

a. Messages classified under OCA will have a justification statement attached to the originating section's file copy. For the Division Headquarters, a copy of the message and the

justification statement will also be maintained by the Division CMCC per the instructions contained in paragraph 6003 of this Order.

b. Messages classified under derivative classification authority will have a listing of source documents attached to the originating section/unit file copy. A sample format for recording classification authority for derivatively classified material is shown at figure 9-2.

2. Material other than messages. All derivatively classified material other than messages require a "Classified by" line, in accordance with reference (c). Samples of properly marked classified documents are shown at figures 9-3 and 9-4.

a. Documents classified under OCA will have a justification statement attached to the originating sections file copy. For the Division Headquarters, a copy of the document and the justification statement will also be maintained by the Division CMCC per the instructions contained in paragraph 6003 of this Order.

b. For documents classified under derivative classification authority, the "Classified by" line must either list a specific source or contain the statement "Multiple Sources". A listing of those sources must be attached to the originating section/unit file copy. A sample format for listing source documents is shown at figure 9-2.

9006. MARKING OTHER CLASSIFIED MATERIAL

1. Maps, Charts and Drawings. The overall classification must be marked at the top and bottom of each document. If the markings might be covered by the customary method of folding or rolling maps, charts and drawings, additional markings that are clearly visible when the document is folded or rolled will be added.

2. Photographs, Transparencies and Slides. When practicable, photographic negatives and positives will be marked with the classification and associated markings and kept in containers that have conspicuous markings. All reproductions of a photograph must clearly show classification and associated markings. For transparencies and slides, the classification and associated markings will be clearly shown on the border, holder or frame and, whenever possible on the image of each transparency or slide.

3. Working Papers. See chapter 10 of this Order for instructions concerning the marking of classified working papers.

4. Transmittals/Cover Letters. When a transmittal document or cover letter is added to classified material, it must carry the highest classification of the information it transmits, and a statement showing the classification, if any, of the transmittal

document standing alone. A sample transmittal/cover letter is shown at figure 9-5.

5. ADP Storage Media. Removeable information storage media and devices (hard drives, 5 1/4 and 3 1/2 diskettes), used with ADP systems, typewriters and word processors, must be labeled using color coded labels (Standard Forms 706, 707, 708, 709, 710 and 711), some of which are shown at figure 9-6. This type of storage media will be marked with the appropriate label even if data stored on it is unclassified. See paragraph 10014 of this Order for more information regarding marking and control of ADP storage media.

6. ADP Systems Marking. Per references (c), (j) and (k), all ADP system components (CPU, keyboard, printer, monitor, etc.) will be marked or labeled to indicate the level of classified material the system is authorized to process. Systems that are only used to process unclassified information will also be marked. Marking/labeling will be accomplished using the labels shown at figure 9-6. If labels shown at figure 9-6 are not available due to being "not in stock" at DSSC, 1" X 3" pressure tape labels may be used until appropriate labels can be procured.

7. Documents Produced by ADP Equipment. Per paragraphs 9-3 and 9-20 of reference (c), products produced by ADP equipment will be have classification and restriction markings applied in the manner outlined below.

a. Overall classification placed at top and bottom center of the front cover (if any), the title page, (if any) and the first page.

b. Downgrading and declassification instructions appear only on the face of the document.

c. Warning notices will be spelled out on the face of the document only.

e. Intelligence control markings will be spelled out on the front cover (if any), title page (if any) and the first page.

f. If a back cover is used, the overall classification is placed at the top and bottom center.

8. Miscellaneous Material. Material such as rejected copy, one-time typewriter/printer ribbons, carbons and reproduction overruns developed in connection with the handling, processing, production and the utilization of classified information will be handled in a manner which ensures adequate protection of the classified information involved and will be destroyed at the earliest practicable time. This material need not be stamped or marked to show level of classification. The exception to this guidance is one-time typewriter/printer ribbons which may be used

to produce several different classified products. These ribbons will be marked with the highest level of classified information contained on them and stored in appropriate security containers when not in use.

9007. SPECIAL ACCESS PROGRAM MATERIAL. Additional restrictions or warning markings, as prescribed by appropriate directives, regulations and instructions relating to approved special access programs, will be applied to material containing information subject to the special access program.

SOP FOR IPSP

SECRET SECRET

FROM CNO WASHINGTON DC
TO CINCPACFLT PEARL HARBOR HI

SECRET //NOFORN//

SAMPLE CLASSIFIED MESSAGE (U)

3. (U) CLASSIFIED MESSAGES WILL BE PARAGRAPH/SUBPARAGRAPH MARKED THE SAME AS NAVAL LETTERS.

4. (U) A "CLASSIFIED BY" LINE IS NOT REQUIRED. THE LAST LINE WILL SHOW, IN ORDER, DOWNGRADING DATA IF APPROPRIATE, THE ABBREVIATED DECLASSIFICATION DATE, OR THE NOTATION "OADR".

5. (U) THE ORIGINATOR'S RECORD COPY WILL INDICATE THE FULL DOWNGRADING/DECLASSIFICATION MARKING AS FOR A DOCUMENT OR LETTER, INCLUDING SOURCES OF DERIVATIVE CLASSIFICATION. THE LAST LINE OF A MESSAGE, HOWEVER, NEED ONLY HAVE THE APPROPRIATE ELEMENTS IDENTIFIED IN PARAGRAPH 2 ABOVE, AS FOLLOWS:

06/C/(DATE) DECL: OADR

SC/NCC/EP

RRS. R. GIBSONS OP-XXE
OP-YYXZ
RR. D. MURRAY S-5555

SECRET

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-1. Sample Properly Marked Classified Message

SOP FOR IPSP

MEMORANDUM

From: (Originating section or individual)
To: File

Subj: CLASSIFICATION AUTHORITY

Ref: (a) (Identify material involved)

1. The reference is classified based on the following sources:
 - a. OPNAVINST S5513.4, enclosure (11)
 - b. OPLAN 5027, Annex B, Appendix 1
 - c. FMFPAC OPORD 201, Annex B, Appendix 1
2. A copy of this memorandum is to be attached to the reference.

I. B. MARINE

Figure 9-2. Sample Format For Recording Classification Authority
For Derivatively Classified Material

SOP FOR IPSP

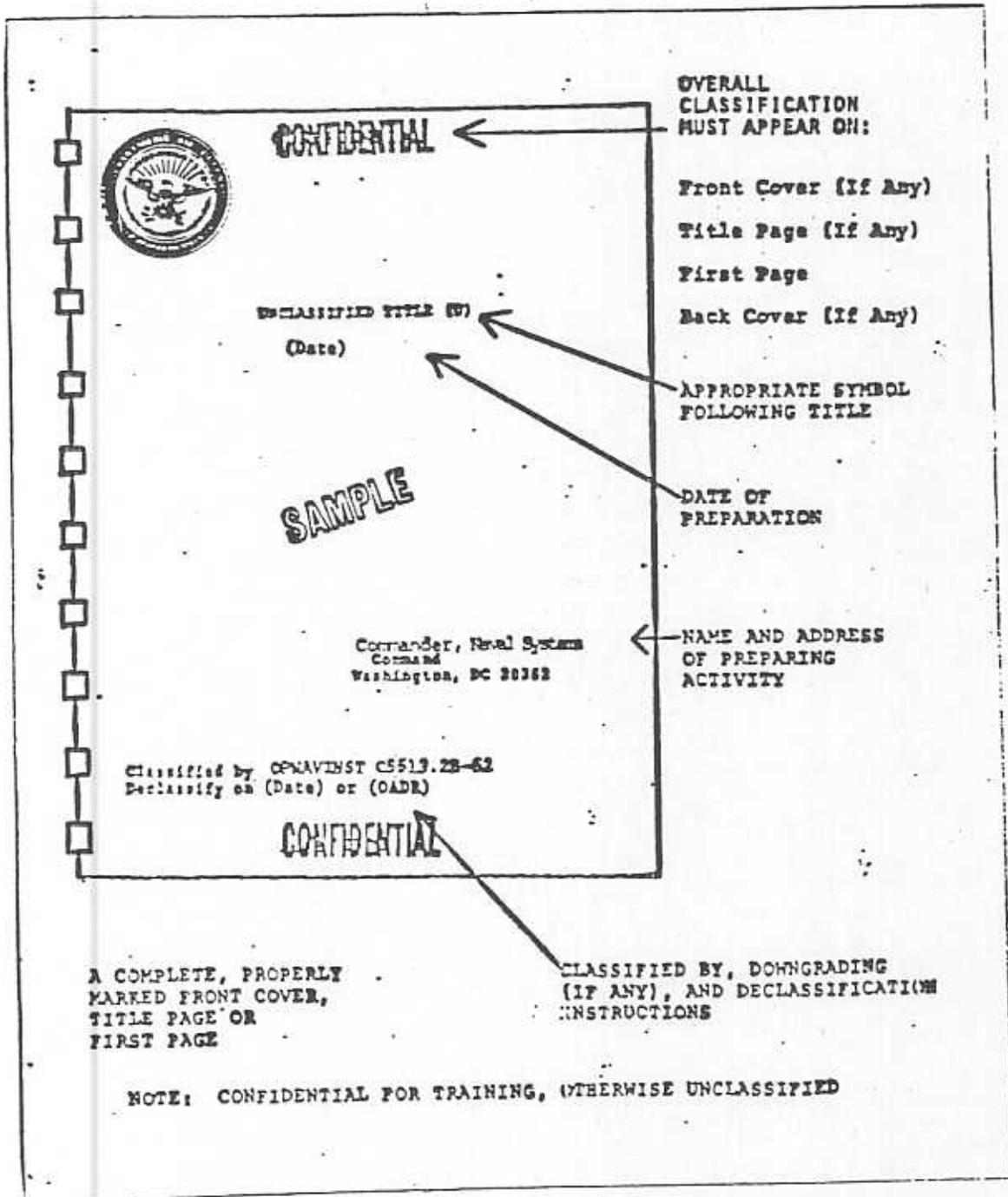


Figure 9-3. Sample Properly Marked Classified Document

SOP FOR IPSP



CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

SS10

Ser III/C123456

Date

CONFIDENTIAL

MEMORANDUM FOR RECIPIENTS

Subj: PORTION MARKING SPECIAL FORMS (U)

1. (U) Mark documents in a manner that eliminates doubt as to which of its portions contains or reveals classified information.
2. (U) There may be occasions when style or format considerations cause an arrangement of words that, standing alone, would not constitute a complete sentence. Normally, such word groups can be revised so as to make a single sentence or paragraph. The following two paragraphs are the same but are arranged differently to illustrate how to apply portion marking.
3. (C) Components of the F-99 aircraft system include:
 - a. a signal processor;
 - b. an emitter module;
 - c. a high frequency receiver; and
 - d. a cryptographic module.
4. (C) Components of the F-99 aircraft system include a signal processor, an emitter module, a high frequency receiver, and a cryptographic module.
5. (U) Subdivisions of the format in 3 above need not be marked if these subdivisions do not constitute a complete sentence. In the stylized format illustrated, there can be no misunderstanding or doubt that everything would be Confidential when taken together.

C. C. BURTON
Head, Security Classification
Management Branch
Security Policy Division

Classified by OPNAVINST 5510.5A-16
Declassify on OADR

CONFIDENTIAL

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-4. Sample Properly Marked Classified Document

SOP FOR IPSP



CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

SSIC - ONLY REFER TO
Ser XII/C123456
(Date)

CONFIDENTIAL--Declassified upon removal of enclosures (1) and (3)

From: Chief of Naval Operations
To: Commander, Naval Systems Command
Subj: SECURITY CLASSIFICATION MARKINGS

Ref: (a) OPNAVINST 5510.1
(b) CNO Washington DC 0123456 Feb 82

Encl: (1) NAVSEA Report 1410, The New Torpedos (U)
(2) List of Attendees
(3) NRL Report 1592, The Principles of Radar (U)

1. When titles or subjects of classified documents are included in the reference line, enclosure line or body of the letter, the classification of the title or subject follows, as shown on the enclosure line above. It is not necessary to show the classification of the reference or enclosure itself; however, each classified enclosure which must be removed before the letter of transmittal can be unclassified must be identified at the top, as shown.

2. Only the first page of an unclassified letter of transmittal carries classification markings. There would be no downgrading and declassification instructions on a letter of transmittal which is itself unclassified. If the letter of transmittal contains classified information, it will carry the appropriate downgrading and declassification instructions for the information it contains.

3. Intelligence control markings are typed out in full at the top, following the classification. If any enclosure contains Restricted Data, Formerly Restricted Data or Critical Nuclear Weapons Design Information, the words should be typed out after the classification at the top and the full warning notice placed at the bottom left. If the letter of transmittal contains information classified at the same level as the enclosure but does not, in itself, contain the information requiring the warning notice or intelligence control marking, words to the effect, "Warning notice (intelligence control marking) cancelled upon removal of enclosure (1)" should appear at the top.

R. R. GORINA
By direction

CONFIDENTIAL

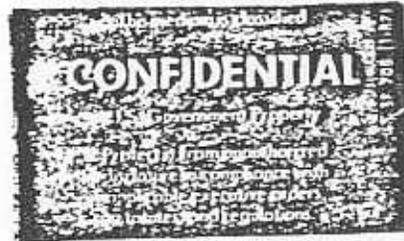
NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-5. Sample Transmittal/Cover Letter

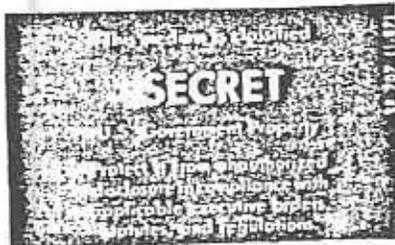
SOP FOR IPSP



Green



Blue



Red



Orange

Figure 9-6. Sample Color Coded Classification Labels

SOP FOR IPSP

CHAPTER 10

ACCOUNTING AND CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	10000	10-3
SCREENING POINTS.....	10001	10-3
TOP SECRET MATERIAL.....	10002	10-3
DOCUMENT REGISTER/LOG.....	10003	10-4
SECRET RECEIPT AUTHORIZATION.....	10004	10-5
RECEIPTS.....	10005	10-5
MASTER LOCATOR FILE.....	10006	10-6
REGISTER/LOG DEAD FILE.....	10007	10-6
RECORDS RETENTION.....	10008	10-6
WORKING PAPERS.....	10009	10-6
WORKING PAPERS CONTROL LOG.....	10010	10-7
CONTROL OF SECRET MESSAGES.....	10011	10-8
CONFIDENTIAL MATERIAL.....	10012	10-8
NAVAL WARFARE PUBLICATIONS.....	10013	10-8
OTHER REQUIREMENTS.....	10014	10-9
ADP STORAGE MEDIA.....	10015	10-9
WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM (WWMCCS) OUTPUT PRODUCTS.....	10016	10-10

FIGURE

10-1	OPNAV 5511/13 RECORD OF DISCLOSURE FOR TOP SECRET MATERIAL.....	10-12
10-2	RECEIPT AUTHORIZATION FORM.....	10-13
10-3	OPNAV 5511/10 RECORD OF RECEIPT.....	10-14
10-4	OPNAV 5216/10 CORRESPONDENCE/MATERIAL CONTROL FORM.....	10-15

SOP FOR IPSP
CHAPTER 10
ACCOUNTING AND CONTROL

	<u>PAGE</u>
FIGURE	
10-5 WORKING PAPERS COVER SHEET.....	10-16

SOP FOR IPSP

CHAPTER 10

ACCOUNTING AND CONTROL

10000. BASIC POLICY. Classified material within the Division will be afforded appropriate accountability and control commensurate to its assigned classification levels to limit dissemination, prevent unnecessary reproduction, and determine responsibility for notification of unscheduled changes or situations of compromise of the information.

10001. SCREENING POINTS. All unit mail rooms and supply sections that receive bulk shipments are designated as initial screening points for classified material. When classified material is received and identified, it will be delivered unopened to the unit adjutant/CMCC immediately for control, distribution and/or storage. Because of the potential for access to classified material, personnel who are assigned to initial screening points will have been the subject of a favorably adjudicated Entrance National Agency Check (ENTNAC) and be U.S. citizens.

10002. TOP SECRET MATERIAL

1. The Division Top Secret Control Officer (TSCO) and all subordinate unit TSCO's will ensure that any top secret document originated or received is entered into the unit's Top Secret accountability register/log. The Top Secret register/log will:

- a. Completely identify the document, including any changes.
- b. Identify the number of copies and disposition for each.

Top Secret registers/logs will be maintained on file for five years after the document is transferred, downgraded, or destroyed. Only top secret material will be recorded in the Top Secret register/log. Specific items of information to enter into the register/log, are contained in paragraph 10003.

2. Each copy of a top secret document will be serially numbered, when originated, with the annotation:

"Copy ____ of ____ copies."

3. Each top secret document will contain a list of effective pages which includes a Record of Page Checks, and every page will be numbered using the annotation:

"Page ____ of ____ pages."

The TSCO will conduct a page check of all top secret documents upon initial receipt and whenever a change involving page entry or removal is accomplished.

4. All top secret holdings will be physically verified at least annually during January, including certificates of destruction and transfer receipts.
5. Retention of top secret material will be kept to the minimum necessary to meet operational needs. Top secret materials will be destroyed as soon as their purpose has been served. Whenever top secret material is destroyed, a record of destruction OPNAV 5511/12, see chapter 17 for example, identifying the material and the two officials who witnessed the destruction will be maintained for two years.
6. All top secret material will be accounted for using a continuous chain of receipts (see chapter 15 for example), and a record of disclosure, for each top secret document maintained.
7. TSCOs will maintain a disclosure record that shows the document title, names of all individuals who have had access to the document, and the date of access. Records of disclosure, (OPNAV 5511/13) shown at figure 10-1, will be retained for two years after the material is destroyed, transferred, or downgraded.
8. Top secret material will not be reproduced without the consent of the originator or higher authority.

10003. DOCUMENT REGISTER/LOG

1. Records will be maintained on top secret, secret and special access (i.e., JCS, NATO, etc.) classified documents, top secret messages, some secret messages (see paragraph 10011) and shall contain, at the minimum, the following information:
 - a. Division/unit control number (assigned by CMCC).
 - b. Date received.
 - c. Control number of organization from which material was received (not required at SCP and SCCP).
 - d. Registered mail number (not required at SCP and SCCP).
 - e. Originator.
 - f. Document date.
 - g. Unclassified title (if classified title, enter "Classified Title").
 - h. Classification of document (not required at SCCP).
 - i. Downgrading instructions (not required at SCCP).

- j. Copy number.
- k. Document serial number (if applicable) (not required at SCP and SCCP).
- l. Total number of pages (top secret only, not required at SCP or SCCP for secret).
- m. Enclosures (not required at SCCP).
- n. Location/Destruction Record (not required/authorized at SCCP).

2. The location/destruction record column should be used to identify what SCP has possession of the material. If the column is left blank, CMCC holds the material.

3. If S-2/G-2 holds the material, enter S-2/G-2 in pencil. If material is mis-routed the pencil entry is easily erased and corrected. The destruction entry will be made in ink and identify the date of destruction. The practice of lining out material that has been destroyed is NOT authorized.

4. CMCC control registers/logs will not be used as a record of receipt for transferring documents from CMCC to another CMCC or to subordinate SCPs, see paragraph 10005 for further guidance.

5. Each classified document will be recorded individually in CMCC/SCP control registers/logs. Multiple copies of the same document will have the same control number, but be marked with different copy numbers (i.e., 1 of 10, 2 of 10, etc.), see paragraph 10006 below for more guidance.

10004. SECRET RECEIPT AUTHORIZATION. Only SCPC, SCPA and personnel designated in writing by the security manager and Heads of General and Special staff sections, are authorized to receipt for classified material from the CMCC using figure 10-2. Receipt authorization is not authorized for personnel who have not been granted appropriate clearance and access.

10005. RECEIPTS. When permanently transferring classified material from CMCC to CMCC or an organization outside the Division, a record of receipt OPNAV 5511/10 form, figure 10-3, will be prepared and a copy retained in a suspense file until the original receipt is received from the unit/organization to which the material was sent. Receipts will be retained for two years. Internally, some units of the Division may find the use of OPNAV 5216/10, figure 10-4, serves as a useful tool for routing classified material within/between headquarters sections. Part 2 of OPNAV 5216 will be used as an internal method of receipt or transfer of classified material from the unit CMCC to subordinate SCPs. OPNAV 5216/10 will not be used to permanently transfer classified material outside the Division. Parts 3 and 4 of the

OPNAV 5216/10 may be used for any other internal control procedures desired by the unit.

10006. MASTER LOCATOR FILE. Each CMCC will maintain a master locator file using part 2 of the OPNAV 5216/10. Multiple copies of a document will not be recorded on the same OPNAV 5216/10. Each part 2 of the OPNAV 5216/10 will represent one classified document on charge to the unit CMCC and its subordinate SCPs. The file is also intended as a backup file for automated files maintained by some CMCCs. When a document is permanently transferred or destroyed, its card will be removed from the file and destroyed.

10007. REGISTER/LOG DEAD FILE. Some unit CMCCs may opt to use an automated control register/log for recording all secret material on charge to that unit. A common practice with an automated control register/log is to simply delete the document entry, once the document has been destroyed or permanently transferred outside the unit. Deleting entries from the automated control register/log negates the requirement to maintain control registers/logs for two years as identified in paragraph 10008 and chapter 10 of reference (c). However, if this practice is followed, part 2 of the OPNAV 5216/10 must be maintained two years after destruction or permanent transfer of the document. Automated control registers/logs will not be utilized for top secret material.

10008. RECORDS RETENTION. All ledgers, logs, registers, receipts, burn reports, or similar records used as inventory or control records of classified documents, will be retained for five years for top secret material, and two years for secret material. The last transaction date (last entry made in register/log) will be the first day of the retention period.

10009. WORKING PAPERS

1. Working papers are documents and material, accumulated or created while preparing finished material (i.e., rough drafts). When working papers contain classified information, the accounting and marking requirements prescribed for the classification may be modified. As a minimum, working papers will be:

a. Dated when created (not required for confidential material).

b. Marked on each page with the highest classification of any information they contain.

c. Protected in accordance with the highest classification assigned.

d. Destroyed by appropriate methods, as soon as they are no longer needed.

e. Controlled by CMCC if retained for over 90 days or transmitted outside the unit where prepared. (Example: Working papers prepared by G-3 and passed to 4th Marines must be controlled by Division CMCC and passed to 4th Marines CMCC).

f. Figure 10-5 will be used as a cover sheet when preparing working papers.

g. A list of source document(s) will be created and maintained with classified working papers in accordance with the guidance provided by reference (c) and chapter 9 of this Order.

2. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain top secret information or are:

a. Released by the originator outside the command, transmitted electrically or transmitted through message center channels within the command;

b. Retained more than 90 days from date of origin; or

c. Filed permanently.

10010. WORKING PAPERS CONTROL LOG

1. A unit CMCC or SCP will maintain a secret working papers control log. The log will contain the following information.

a. Control number (i.e. 1-92/G-3).

b. Unclassified title (if classified, enter "Classified Title").

c. Date created.

d. Disposition/Destruction.

(1) Disposition - (i.e., controlled by CMCC as document number _____).

(2) Destruction - (date of destruction; if working papers included material controlled by the unit CMCC or portions of material controlled by CMCC, prepare burn report identifying enclosures destroyed, CMCC will be provided with original burn report SCP will maintain copy).

2. Classified enclosures to working papers should be recorded on a working list attached to the cover sheet. Information to include on the working list is shown below. Whenever possible, this information can be incorporated in the classification source list addressed in paragraph 9005 of this Order.

- a. If message received from servicing communications facility; originator, Date Time Group (DTG), classification, downgrading/declassification instructions.
- b. If message controlled by unit CMCC, CMCC control number, originator, classification and downgrading/declassification instructions.
- c. If portion of classified document reproduced by CMCC, include CMCC control number of original document, originator, classification, downgrading/declassification instructions.

10011. CONTROL OF SECRET MESSAGES

1. Secret messages received from a unit's supporting communications center do not require control by unit CMCCs (message received is "addressed" to receiving unit). The exceptions to this are special access program and NATO information identified in paragraph 1-5 of reference (c).
2. Secret messages received via registered mail, courier, or secure facsimile will be controlled by unit CMCCs. Destruction of these controlled secret messages will be recorded on destruction reports.
3. Secret messages controlled by a unit CMCC will be assigned control numbers just like those assigned to documents. The message Date Time Group (DTG), will not be used as a control number.
4. Secret messages received from the unit's supporting communications center and distributed during a conference, (i.e. Division holds conference with MSCs, which were not action/info addressees, must be controlled by Division CMCC prior to distribution at the conference.

10012. CONFIDENTIAL MATERIAL. Records of receipt, distribution, or disposition for Confidential material are not required. However, administrative provisions to protect confidential information from unauthorized disclosure by controlling access and complying with marking, storage, transmission, and destruction requirements contained in the current edition of reference (c) and this Order will be used.

10013. NAVAL WARFARE PUBLICATIONS. Naval Warfare Publications (NWP) have their own system for administrative controls. NWPs that are classified must be handled according to the access, accountability, storage, transmission and destruction requirements for their particular level of classification in accordance with the provisions contained in the current edition of references (c) and (h).

10014. OTHER REQUIREMENTS. Additional accounting and control requirements for special categories of classified material are contained in the following directives:

1. COMSEC material - Cryptographic Security Policy and Procedures CSP-1, and Communications Material Systems Manual (CMS-4), references (d) and (e).
2. Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI) - OPNAVINST S5511.35J.

10015. ADP STORAGE MEDIA

1. Removeable hard drive. A removeable hard drive used to prepare and store classified information, will be protected and stored in accordance with established procedures for the highest level of classification of information recorded on the drive. The following additional procedures will be adhered to;

a. Top secret information will not be recorded on removeable hard drives.

b. A removeable hard drive will be marked with a pressure tape label with the words "Working Papers" printed or stamped on the label using red ink. The drive will also be marked with an appropriate classification label as outlined in paragraph 9006 of this Order.

2. Diskettes. Diskettes (5 1/4" and 3 1/2") used to prepare and store classified information, will be protected and stored in accordance with established procedures for the highest level of classification of information recorded on the drive. The following additional procedures will be adhered to;

a. Classified information will be recorded on an appropriately colored diskette.

- (1) Top Secret - orange.
- (2) Secret - red.
- (3) Confidential - blue.
- (4) Yellow - SCI (SCIF only).

b. Diskettes used to record classified information that are not of the colors identified above, will be marked with the appropriate classification labels identified in paragraph 9006 of this Order. The diskette will also be marked with a pressure tape label with the words "Working Papers" printed or stamped on the label using red ink.

c. Yellow diskettes will only be used by the Division SCIF. The exception to this rule will be those diskettes that are readily identified as containing manufacture software. Unit security managers will confiscate and take appropriate action for all other yellow diskettes.

3. Unit CMCCs will make every effort to procure (from DSSC) and stock adequate quantities of appropriately colored diskettes for use in recording classified material. Orange diskettes will be controlled by the TSCO in accordance with established procedures for top secret material. Red diskettes will be controlled by the unit CMCC in accordance with established procedures for the protection of secret material. Controlled red diskettes will be issued to SCPs for use in the preparation and storage of secret information. Until such time as adequate stocks of red diskettes are available from DSSC, diskettes used to prepare and store Secret information will be marked according to the directions contained in this paragraph. When adequate amounts of red diskettes are available for use, secret information contained on diskettes of other colors will be transferred to the red diskettes and the old diskettes will be destroyed in accordance with the instructions contained in reference (c) and chapter 17 of this Order.

10016. WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM (WWMCCS)
OUTPUT PRODUCTS

1. Records of WWMCCS output products will be maintained per references (q) and (p), as long as the products remain within the confines of the WWMCCS spaces.
2. Teleconferencing (TLCF) and File Transfer Service (FTS) messages removed from WWMCCS spaces, will be protected and controlled according to the highest level of classified information contained in the message. TLCF and FTS messages will be destroyed as soon as they have served their intended purpose by a means approved for the destruction of the highest level of classified information contained in the message.
3. Joint Operation Planning & Execution System (JOPES) and Timed Phased Force Deployment Data (TPFDD) documents removed from the WWMCCS spaces, will be treated as classified working papers and protected according to the highest level of classified information contained in the document. All confidential and secret WWMCCS working papers will be destroyed as soon as they have served their intended purpose, by a means approved for the destruction of the highest level of classified information contained in the document.
4. Secret WWMCCS working papers will be logged into a working papers log maintained by the G-3 SCP custodian. Entries in the log will include the following information:

- a. Control number (WWMCCS 1-92).
- b. Date created (date removed from WWMCCS spaces).
- c. Unclassified title (if classified enter "Classified Title").
- d. Classification, restrictions or warning notices (S/NF).
- e. Classification authority.
- e. Downgrading/declassification instructions.
- f. Disposition/destruction date.

Secret WWMCCS working papers retained for more than 90 days will be controlled by the Division CMCC. The entry in the disposition column of the working papers log, will be the control number assigned to the document by CMCC. The date of destruction will be entered in the Disposition/Destruction column for SECRET WWMCCS working papers destroyed before the 90 day limitation.

5. Top secret products received via the WWMCCS terminal for the 3d Marine Division, will immediately be delivered to the Division TSCO for control and appropriate disposition.

SOP FOR IPSP

ACTIVITY:				DATE:
DD HAS DIV RECEIPT AUTHORIZATION RECORD FOR CLASSIFIED MATERIAL			DD HAS DIV FORM 5511-6 (9-85)	
<ol style="list-style-type: none"> 1. The personnel listed below, are authorized to receipt for classified material up to and including the level of classification entered in the level of receipt column. 2. It has been certified that these personnel have to appropriate clearance necessary. 3. All previous authorizations are hereby cancelled. 				
NAME	SSN	NAME	LEVEL OF RECEIPT	SIGNATURE
AUTHORIZING OFFICIAL:			SIGNATURE:	

Figure 10-2. Receipt Authorization Form

SOP FOR IPSP

OPNAV 5511/10 REC'D 5/8 1974 (20-111)		RECORD OF RECEIPT OPTIONAL FORM NO. 10				THIS RECEIPT MUST BE RECORDED AND RETURNED
ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF RECEIPT	ENCLOSURE DESCRIPTION	COPIES MADE	NO. OF COPIES TO BE RETURNED	RECEIVED CLASSIFICATION
Op-XXX	812345	(Date)	Security Classification Guide	1	1	
RECEIVED BY (Name in Block) CNO Op-XXX31 SIGNATURE (Typed Name)				DATE (Date)		

Figure 10-3. OPNAV 5511/10 Record Of Receipt

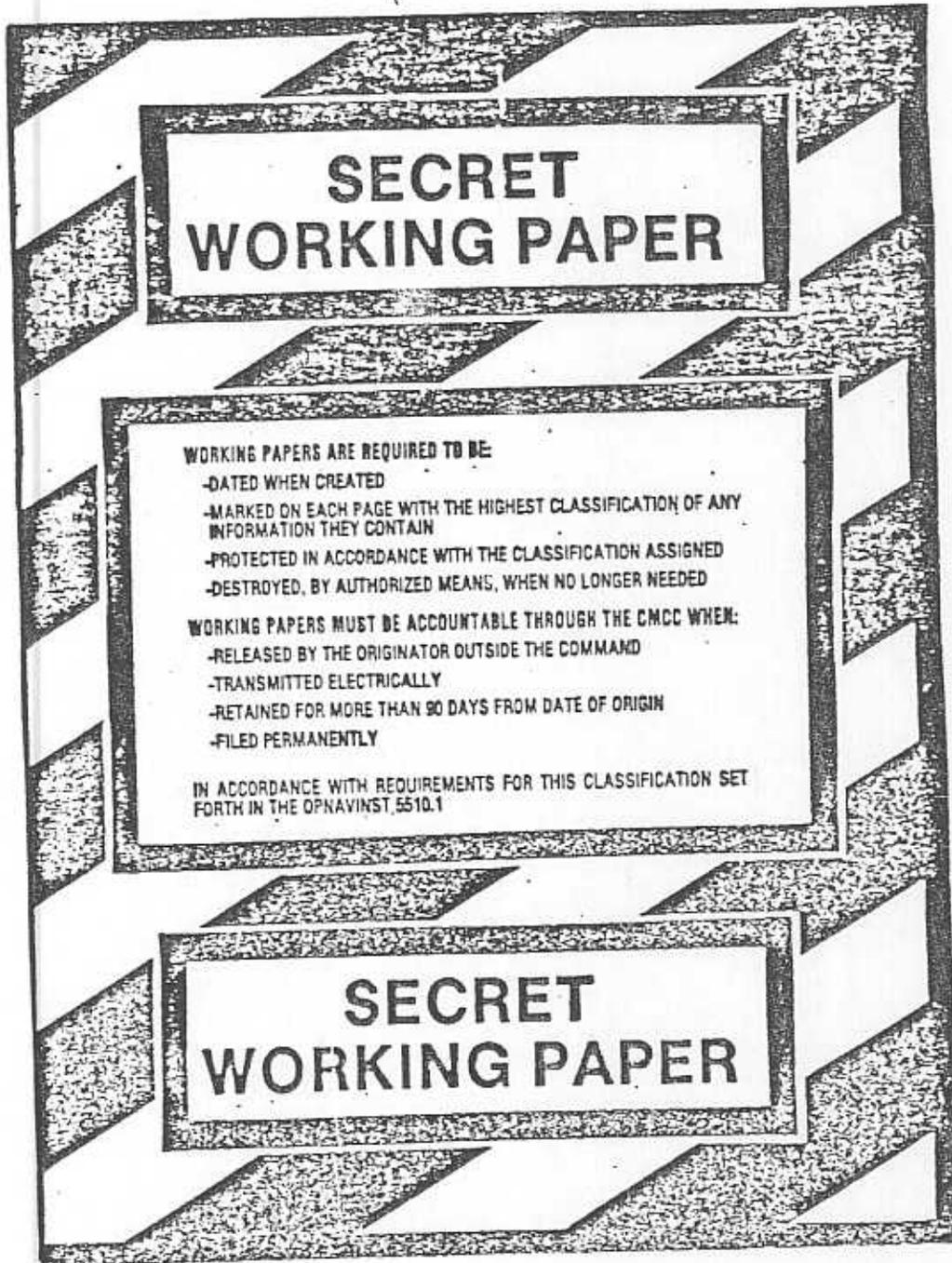


Figure 10-5. Working Papers Cover Sheet

SOP FOR IPSP

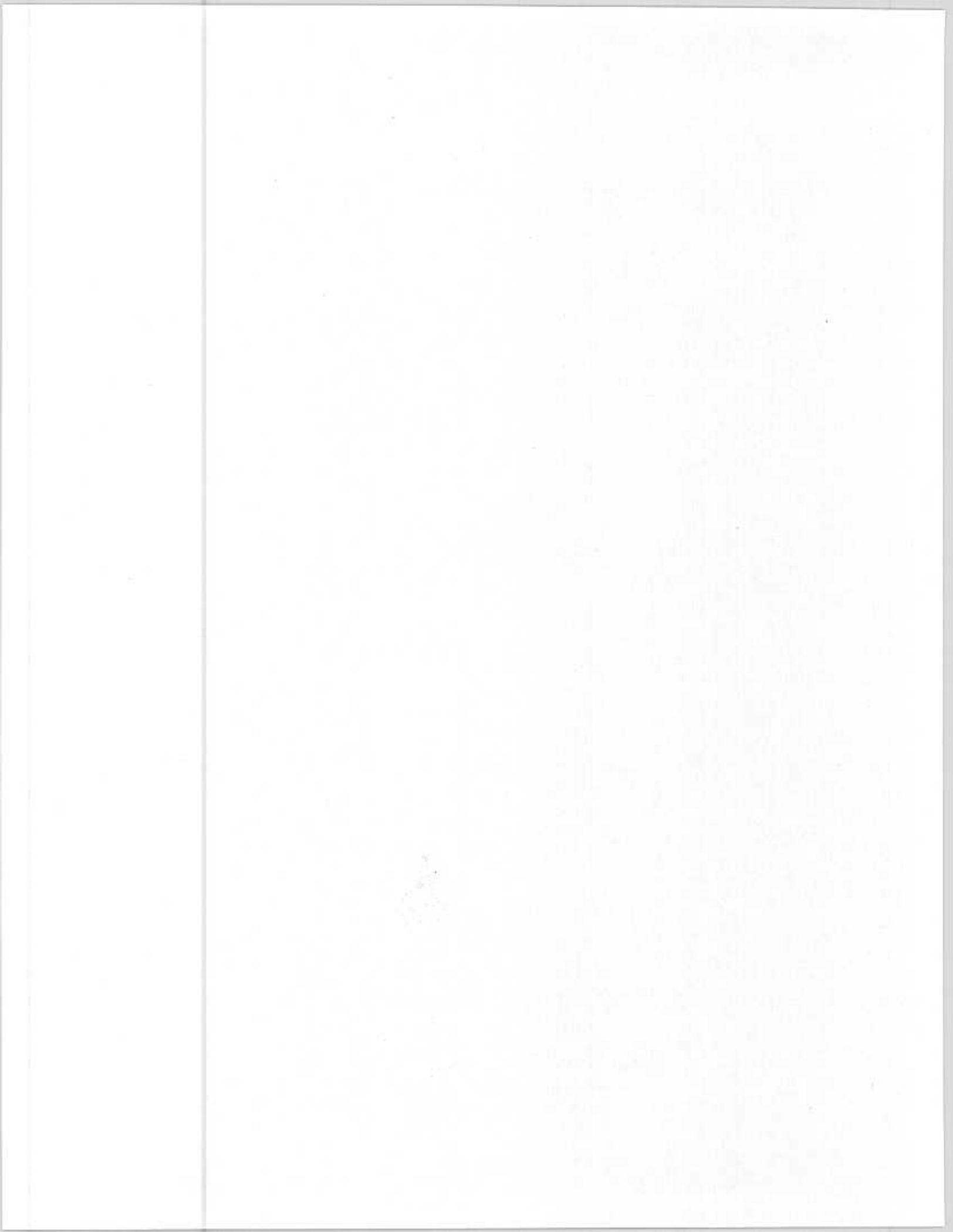
CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	11000	11-3
REPRODUCTION CONTROL LOG.....	11001	11-4
REPRODUCTION EQUIPMENT.....	11002	11-5
CONTROL OF PHOTOGRAPHY.....	11003	11-5
ARTISTS, SKETCHERS AND DRAFTSMAN.....	11004	11-7
TELECOPIERS.....	11005	11-7

FIGURE

11-1	SAMPLE WARNING SIGN FOR REPRODUCTION EQUIPMENT.....	11-8
11-2	SAMPLE WARNING SIGN FOR REPRODUCTION EQUIPMENT.....	11-9



SOP FOR IPSP

CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

11000. BASIC POLICY. No classified material will be reproduced by any means unless authorized by the appropriate official listed below. Every effort must be made to minimize the reproduction of classified material.

1. Top Secret. Top secret information (documents and messages) will not be reproduced without the consent of the originating activity or higher authority. Requests for the reproduction of top secret material will be submitted to the Commanding General, via the Division Security Manager in writing. The request will include a detailed description of the material and justification for its reproduction.

2. Secret Documents. The reproduction of secret documents must be authorized by the unit's reproduction control officer or in his absence, the unit security manager. The material will be reproduced by two appropriately cleared personnel. One of those personnel must be a member of the unit's CMCC. Records of the reproduction will be maintained by CMCC per the instructions contained in paragraph 11001.

3. Secret Messages. The reproduction of secret messages controlled by the unit CMCC must be authorized by the unit's reproduction control officer or in his absence, the unit security manager. The material will be reproduced by two appropriately cleared personnel. One of those personnel must be a member of the unit's CMCC. Records of the reproduction will be maintained by CMCC in accordance with the instructions contained in paragraph 11001. Heads of General and Special Staff sections of the Division Headquarters may authorize the reproduction of secret messages under the following conditions;

a. The message was received from the Division Communications Center.

b. The message is intended for section internal use only.

c. The section has been authorized and maintains a Secondary Control Point (SCP).

4. Confidential Documents/Messages. The reproduction of confidential documents and messages will be accomplished in accordance with the restrictions contained in reference (c). Confidential documents and messages which are marked with restrictions outlined in paragraph 9-32 of reference (c), will either not be reproduced, or will be reproduced only after receiving the appropriate approval from the originator or higher authority. Confidential documents or messages which do not contain restrictions outlined in paragraph 9-32 of reference

(c), may be reproduced with the approval of the unit's reproduction control officer or in his absence, the unit security manager. The unit CMCC will maintain a record of the confidential documents or messages with restrictions, reproduced per the instructions contained in paragraph 11001. Heads of General and Special Staff sections of the Division Headquarters, may authorize the reproduction of confidential messages under the same conditions identified for secret message reproduction addressed in paragraph 11000.3, if the message is not covered under the restrictions identified in paragraph 9-32 of reference (c). Dissemination of reproduced documents and messages will be accomplished per the instructions contained in chapter 11 of reference (c) and this Order.

5. Individuals authorized to approve the reproduction of any classified material are responsible for ensuring that all original classifications markings and restrictions are carried forward to the reproduced material.

11001. REPRODUCTION CONTROL LOG

1. Top Secret. Reproduced top secret material will be controlled and records maintained per the instructions contained in chapter 10 of reference (c).

2. Secret and Confidential Documents. The secret and confidential document reproduction control log will be maintained by the unit CMCCO. Entries in the log will include the following information;

a. CMCC control number of original document. (Not applicable for Confidential material)

b. Copy number of original document. (Not applicable for Confidential material)

c. Originator of original document.

d. Classification and restrictions of original document.

e. Downgrading/Declassification instructions of original document.

f. Number of copies produced.

g. Actual material reproduced (i. e. "all" of document or identify specific pages or enclosures).

h. Identify new CMCC control number and copy number(s) applied to the reproduced material, (if 2 copies are reproduced, documents should be assigned copy numbers 1 of 2 and 2 of 2). If reproduced material is intended for inclusion in working papers, identify unit/section working papers control number. (Not

applicable for confidential material unless paragraph 9-32 of reference (c) restrictions apply)

i. Signature of reproduction control officer or security manager.

3. Secret and Confidential Messages. The unit's CMCC will maintain the secret and confidential message reproduction control log. Secret messages that require reproduction control by a unit's CMCC are identified in paragraph 10011. Confidential messages that require reproduction control by a unit's CMCC are identified in paragraph 9-32 of reference (c). Entries in the reproduction control log will include the following information:

- a. Originator of message.
- b. Date Time Group (DTG) of message.
- c. Classification and restrictions of message.
- d. Downgrading/Declassification instructions.
- e. Number of copies reproduced.

f. Signature of reproduction control officer, unit security manager.

11002. REPRODUCTION EQUIPMENT. To the extent possible, controlled areas for reproduction of classified material will be established. At a minimum, the reproduction equipment authorized for reproducing classified material will be specifically designated and signs will be prominently displayed both on and near the equipment to advise users of restrictions. Signs may read for example, "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY (designated official)." "All" machines that are not authorized for the reproduction of classified material will be posted with a warning notice such as "THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL." Reproduction machines will be located in areas that are easily observable to ensure that only authorized copies are being made and the number of copies is kept to a minimum. Sample warning signs that may be used within the 3d Marine Division are shown at figures 11-1 and 11-2. The date the sign is posted will be included on the sign, along with the signature of the unit security manager. Unit security managers will ensure that all reproduction machines are checked for warning signs during monthly after hours security inspections.

11003. CONTROL OF PHOTOGRAPHY

1. Commanding officers are responsible for controlling photography within their commands. Commanding officers will publish in chapter 25 to this Order, adequate guidance and

restrictions for photography within their areas of responsibility if considered necessary.

2. It is the responsibility of every member of this Division to question anyone, military or civilian, observed taking photographs of what are known or suspected restricted subjects. If it cannot be determined that the photography is authorized, the incident must be reported to the unit security manager or Command Duty Officer immediately. Individuals observed taking photographs of areas where photography is prohibited both by directive and posted signs, are subject to being detained until their status is determined, and their photographic negatives are liable to confiscation. All incidents involving detention or confiscation will be reported to the Division Security Manager.

3. Requests to photograph facilities or equipment not listed below by military personnel, civilians, media and commercial photographers, will be submitted to the appropriate unit security manager. Authorization will be granted in writing and an escort will be assigned to accompany the photographer(s).

4. Authorized Photography. Personnel of the Division and MSCs are authorized to have photographic equipment in their possession and to take photographs of unclassified facilities subject to the provisions of reference (c) and this Order. Photography is approved in the following general areas within the environs of the Division:

- a. Athletic fields.
- b. Post Exchange/Club facilities.
- c. Special Services activities and facilities.
- d. Designated "Open House" activities, within specified areas.
- e. Within an office space for award presentations or ceremonial events.

5. Unauthorized Photography. The following are considered unauthorized photography:

- a. Photography of classified material.
- b. Photography taken inside an office space or command post where classified material is being displayed.
- c. Photography of communications facilities and associated physical security arrangements.
- d. Photography of armories and associated physical security

arrangements.

11004. ARTISTS, SKETCHERS AND DRAFTSMAN. The security controls for photography are also applicable to artists, sketchers and draftsman.

11005. TELECOPIERS. Telecopiers, facsimile transmitters, etc., that use unsecure telephone systems will not be used to receive or transmit classified material.

SOP FOR IPSP

SECURITY NOTICE

1. THIS MACHINE IS AUTHORIZED FOR THE REPRODUCTION OF SECRET AND CONFIDENTIAL CLASSIFIED MATERIAL.
2. PRIOR TO ANY CLASSIFIED REPRODUCTION, AUTHORIZATION MUST BE OBTAINED FROM THE CLASSIFIED MATERIAL CONTROL OFFICER, ROOM: _____, BLDG: _____, EXT: _____.
3. REPRODUCED COPIES OF CLASSIFIED DOCUMENTS ARE SUBJECT TO THE SECURITY CONTROLS PRESCRIBED FOR THE ORIGINAL DOCUMENT.
4. REPRODUCED MATERIAL SHALL SHOW OR BE MARKED TO SHOW THE CLASSIFICATION AND OTHER SPECIAL MARKINGS WHICH APPEAR ON THE ORIGINAL MATERIAL.
5. SAMPLES, WASTE OR OVERLAYS RESULTING FROM THE REPRODUCTION PROCESS SHALL BE SAFEGUARDED ACCORDING TO THE CLASSIFICATION OF THE INFORMATION INVOLVED, AND SHALL BE DESTROYED PROMPTLY AS CLASSIFIED WASTE.

DATE POSTED AND SIGNATURE _____

Figure 11-1. Sample Warning Sign For Reproduction Equipment

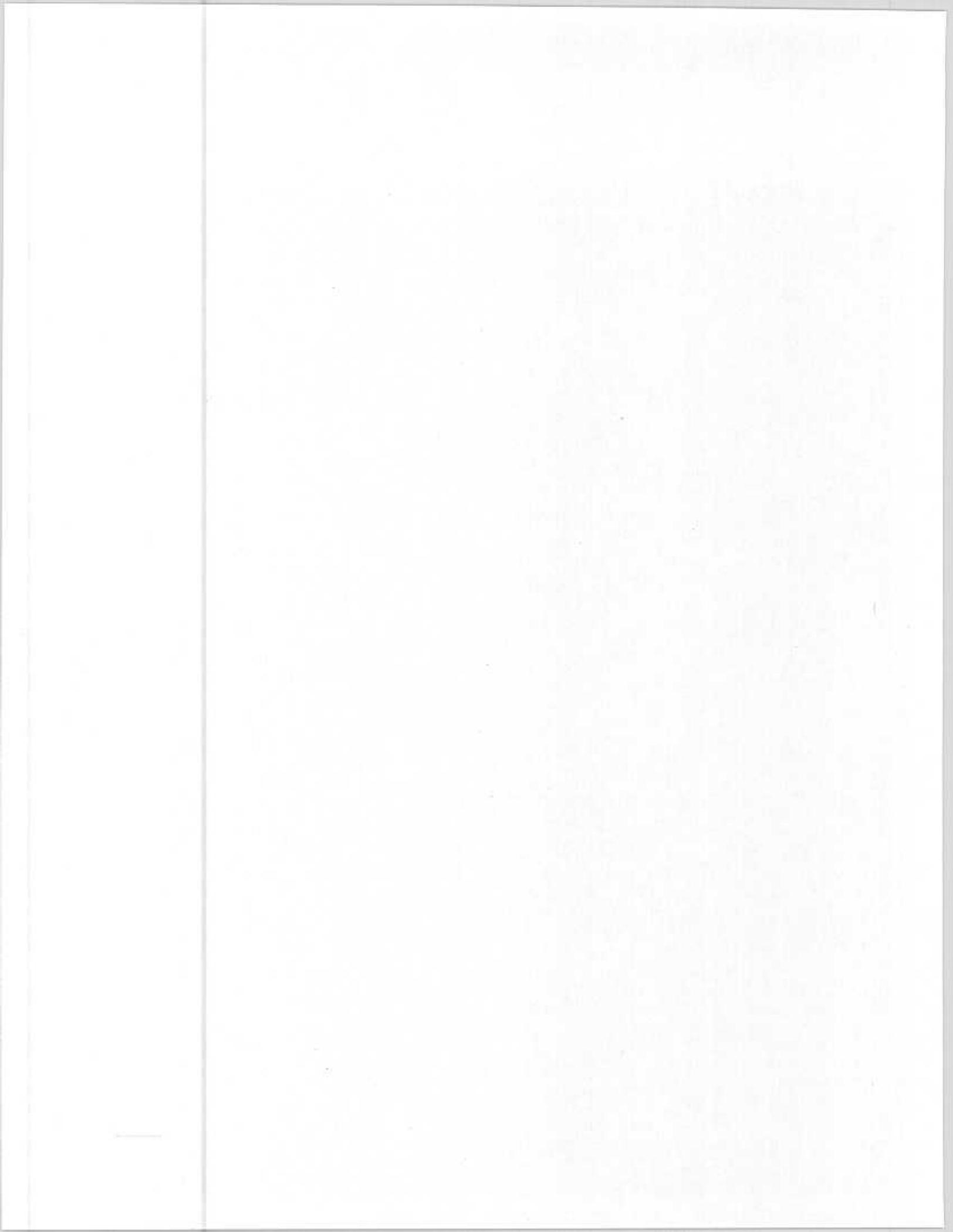
SOP FOR IPSP

SECURITY NOTICE

1. THIS MACHINE IS NOT AUTHORIZED FOR THE REPRODUCTION OF ANY CLASSIFIED MATERIAL.
2. AUTHORIZATION FOR, AND THE REPRODUCTION OF CLASSIFIED MATERIAL MUST BE OBTAINED FROM, AND ACCOMPLISHED BY THE CLASSIFIED MATERIAL CONTROL OFFICER, ROOM: _____
BLDG: _____, EXT: _____.

DATE POSTED AND SIGNATURE

Figure 11-2. Sample Warning Sign For Reproduction Equipment

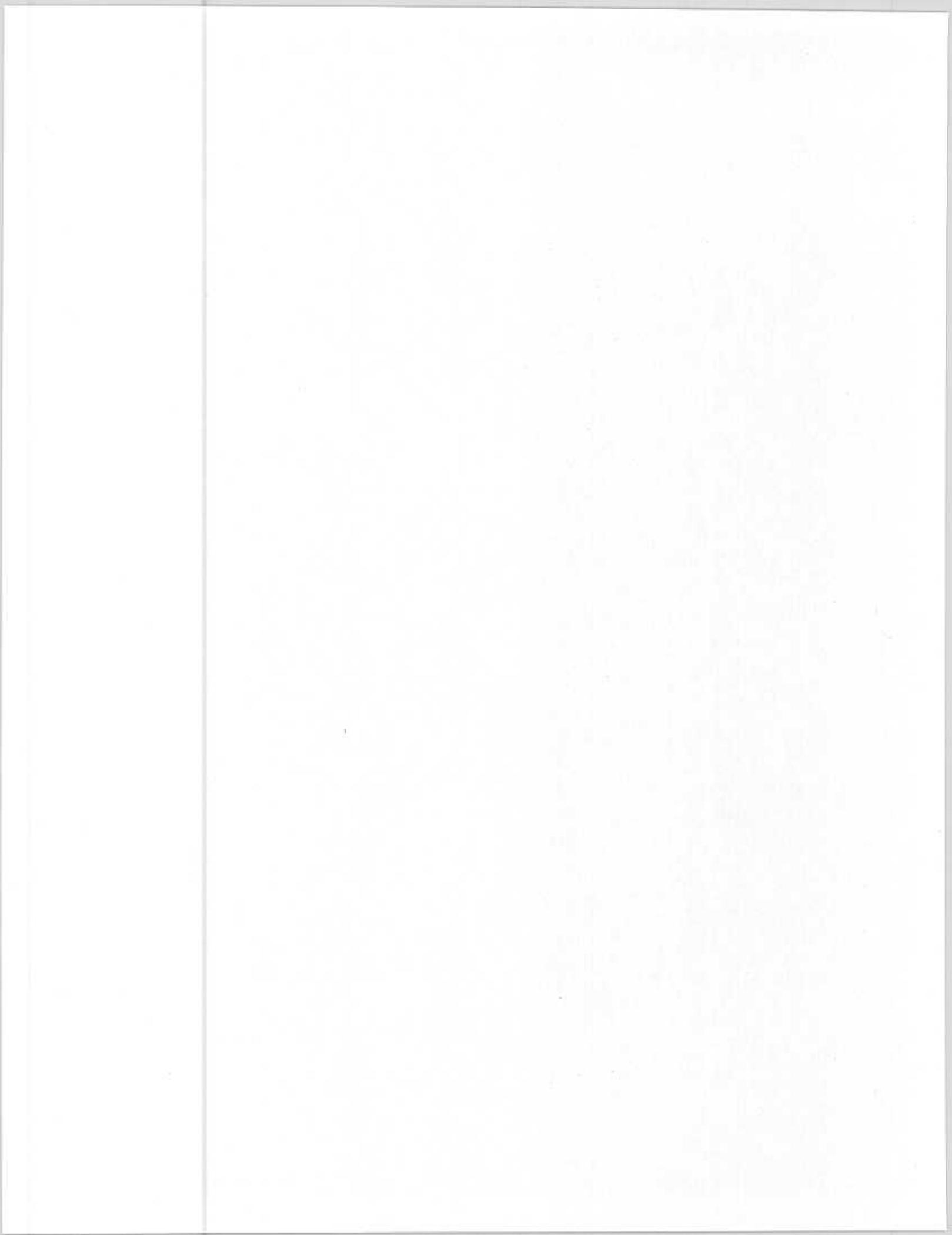


SOP FOR IPSP

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	12000	12-3
MATERIAL FOR PUBLIC RELEASE.....	12001	12-3
SPECIAL ACCESS PROGRAM MATERIAL.....	12002	12-3
TOP SECRET MATERIAL.....	12003	12-3
SECRET DOCUMENTS.....	12004	12-4
SECRET MESSAGES.....	12005	12-4
CONFIDENTIAL DOCUMENTS AND MESSAGES.....	12006	12-4



SOP FOR IPSP

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

12000. BASIC POLICY. Dissemination of classified material within the Division will be limited to those activities possessing a valid need to know and will reflect any restrictions imposed by originators or higher authority. Dissemination of classified material to activities outside the Division will be in accordance with chapter 12 of reference (c) and this Order.

12001. MATERIAL FOR PUBLIC RELEASE. Commanding officers will ensure that material prepared or submitted for public release does not contain classified information. Policies and procedures governing public release of official information and circumstances under which security review is required are detailed in SECNAVINST 5720.44A and MCO 5510.9A.

12002. SPECIAL ACCESS PROGRAM MATERIAL. Special Access Program material will be disseminated in accordance with current directives applicable to that program. Programs and applicable directives are listed below:

1. Restricted Data and Formerly Restricted Data, see the current edition of DOD 5210.2.
2. NATO material, see the current edition of OPNAVINST C5510.101D.
3. Cryptographic information, see the current editions of CMS 4 and CSP-1.
4. SIOP information, see the current edition of OPNAVINST S5511.35.
5. For other special access program information not covered by reference (c) or this Order, direct all questions to the Division Security Manager.

12003. TOP SECRET MATERIAL. Top secret material, including messages, will not be disseminated outside the Division without the consent of the originator, higher headquarters or the Commanding General, 3d Marine Division.

1. Top secret messages received by the Communications Center and intended for the 3d Marine Division, will be processed in accordance with the guidance contained in paragraph 2004 of reference (u). Communications Center personnel will not deliver the message to the TSCO. The TSCO or alternate will pickup and receipt for the message from the Communications Center. The top secret message will be transported to the CMCC/CMS spaces for control and appropriate disposition.

2. The dissemination of top secret material will be kept to the absolute minimum. Whenever possible, top secret material will be read or utilized inside the confines of the CMCC/CMS spaces where it is stored.

3. If it is necessary to disseminate top secret material within the Division Headquarters, it will be delivered directly to the person who is to assume responsibility for it. The material will have the appropriate disclosure sheet attached, and the person assuming responsibility will sign a receipt for the material. Top Secret material will be returned to its authorized storage area prior to the close of business that same working day.

12004. SECRET DOCUMENTS. Secret documents may be disseminated within and to organizations outside the Division per reference (c) and this Order, unless specifically prohibited by the originator or higher headquarters. All secret documents (including working papers) disseminated within the Division and to or from the Division Headquarters, must be processed through the appropriate Division/unit CMCC. SCPs may only draw and return secret documents to its Division/unit CMCC. SCCPs may only draw and return secret documents from/to its parent SCP. Within the Division Headquarters, heads of General and Special staff sections are authorized to pass secret documents controlled by the Division CMCC and on charge to that SCP, to another General or Special staff section for comment or review for periods not to exceed 48 hours. The General or Special staff section SCP charged with accountability for the Secret document, is responsible for ensuring that the secret document is returned within the time allotted and properly secured while in the physical custody of the other section.

12005. SECRET MESSAGES. Secret messages received from the unit's supporting communication facility may be disseminated within the Division Headquarters or within the headquarters of MSCs to which addressed. Secret messages transmitted and received via registered mail, courier, or secure facsimile will be controlled by the Division/unit CMCC including recording of destruction on OPNAV Form 5511/12.

Example: Secret message received by CG THIRD MARDIV G-2 and needed by 4th Marines S-2, but not addressed to 4th Marines. Message will be controlled and forwarded to 4th Marines via CMCC channels, or readdressed to 4th Marines via communications facilities.

12006. CONFIDENTIAL DOCUMENTS AND MESSAGES. Within the Division, confidential documents and messages may be passed to units or sections only after it has been determined that the unit/section has a valid need to know, appropriately cleared personnel to receive and transport the material and the unit/section has the proper storage facilities.

SOP FOR IPSP

CHAPTER 13

SAFEGUARDING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	13000	13-3
RESPONSIBILITY FOR SAFEGUARDING.....	13001	13-3
CARE DURING WORKING HOURS.....	13002	13-3
SECURITY CHECKS.....	13003	13-5
AFTER HOURS INSPECTIONS.....	13004	13-5
RANDOM ENTRANCE/EXIT INSPECTION.....	13005	13-6
PROHIBITION AGAINST WORKING ALONE.....	13006	13-6

FIGURE

13-1 TOP SECRET COVER SHEET.....	13-7
13-2 SECRET COVER SHEET.....	13-8
13-3 CONFIDENTIAL COVER SHEET.....	13-9
13-4 SECURITY CONTAINER CHECK SHEET.....	13-10
13-5 ACTIVITY SECURITY CHECKLIST.....	13-11
13-6 UNANNOUNCED AFTER HOURS INSPECTION REPORT.....	13-12
13-7 RANDOM ENTRANCE/EXIT INSPECTION REPORT.....	13-13

SOP FOR IPSP

CHAPTER 13

SAFEGUARDING

13000. BASIC POLICY. Classified information or material will be used only where there are facilities, or under conditions, adequate to prevent unauthorized persons from gaining access to it. To the extent possible, classified holdings will be consolidated to limit the areas where it will be used. The requirements in reference (c) and this Order represent the minimum acceptable standards.

13001. RESPONSIBILITY FOR SAFEGUARDING. Anyone who has possession of classified material is responsible for safeguarding it at all times, and particularly for securing classified material in appropriate security containers whenever it is not in use or under direct supervision by authorized personnel. Classified information will not be removed from designated office spaces or working areas except in the performance of official duties and then only under conditions providing the required protection. Third Marine Division personnel are not authorized to remove classified material from official working spaces and take it to their quarters under any circumstances.

13002. CARE DURING WORKING HOURS. During working hours, the following precautions will be taken to prevent access to classified information by unauthorized persons:

1. When classified documents are removed from storage for working purposes, they will be kept under constant surveillance and face down, or covered when not in use. Cover sheets (figures 13-1, 13-2 and 13-3) or folders corresponding to the level of classification of the material will be utilized.

2. Classified information will be discussed only when unauthorized persons cannot overhear the discussion. Passageways, ladderwells, parking lots and social gatherings are inappropriate for discussing classified material. Particular care should be taken in or around the work area when there are visitors whose clearance and access status is not known.

3. When local nationals are required to perform repairs or maintenance in areas where classified material is used and/or stored, all such material will either be removed from that space, or secured in approved security containers until the work is completed. Local national workers will be under continuous escort when working in spaces authorized for the use and storage of classified material.

4. Preliminary drafts, stenographic notes, working papers and similar material containing classified information, will be protected according to the level of classification of the material from which they were generated. When these items have served

their intended purpose, they will be destroyed by approved methods. These materials will be protected with cover sheets identified in this paragraph and paragraph 10009.

5. Typewriter ribbons and ADP Storage media (removeable hard drives and diskettes) will be safeguarded and marked with the highest classification of material for which they were used. Detailed guidance on computer diskettes and other magnetic storage media can be found in paragraph 10015 of this Order. One-time printer and typewriter ribbons will be destroyed by approved means as classified waste.

6. When transporting classified material from one office to another within the same building, cover sheets or folders identified above will be utilized to protect classified material from unauthorized disclosure. Classified material transported from one building to an adjacent building will be protected by an appropriate cover sheet or folder and carried in a locked briefcase. Transporting classified material further than an adjacent building will be accomplished in accordance with the directions contained in reference (c) and chapter 16 of this Order.

7. During the lunch hour (1130-1300), classified material will be secured in appropriate security containers. The practice of leaving classified material in red baskets and under the supervision of the phone watch is not considered prudent.

8. At the end of each work day, all classified and unclassified waste should be either destroyed per reference (c) and chapter 17 of this Order, or properly safeguarded until it can be destroyed.

9. Combinations of security containers will be committed to memory. Combinations will be recorded and stored in accordance with the instructions contained in reference (c) and chapter 14 of this Order.

10. Only STU-III telephones that are properly keyed, will be used when discussing classified information during telephone conversations. The STU-III must be keyed for the level of classified information being discussed. Individuals must not Talk Around classified information in the unsecured mode using a STU-III or unclassified telephones.

11. The only secure facsimile machine authorized for transmission or receipt of classified material from or to the Division Headquarters is located in the III MEF Command Center. Secret or confidential material intended for transmission via secure facsimile, will be controlled and delivered to the Command Center by Division CMCC personnel only. Actual transmission of the classified material will be performed by Command Center personnel.

12. Unit security managers will ensure that areas where classified material is utilized and/or stored, have limited entrances into the area. Office spaces with multiple entrances will designate one main entrance into the work spaces. Other entrances will remain locked, but not blocked, during normal working hours. The intent is to enhance visitor and access control to those areas where classified material is utilized and/or stored.

13003. SECURITY CHECKS

1. Supervisors will require a security check at the end of each working day to ensure all classified material is properly secured. Figure 13-4 will be attached to each security container and filled in at the end of each day. If the security container was not opened during the course of business that day, after the date, the entry "NOT OPENED" will be entered followed by the persons initials and the time the container was checked. Standard Form 701, Activity Security Checklist, figure 13-5, will be posted near the main entrance to the office spaces and shall be used to record securing the spaces at the end of each work day. The Activity Security Checklist will be utilized for all spaces where classified material is stored.

2. Buildings and office spaces within the 3d Marine Division are subject to inspections both announced and unannounced, during working hours or after working hours, at the discretion of the unit commanding officer.

3. Unit commanding officers will cause duty personnel to check spaces where classified material is stored after normal duty hours. Duty personnel will record their after hours security checks on the posted Activity Security Checklist. Commanding Officers may also required that after hours security checks be recorded in official duty logs.

13004. AFTER HOURS INSPECTIONS. Unit security managers will conduct an internal unannounced after hours security inspection. This inspection will be conducted at least once each month. Unit duty personnel will be informed when this inspection begins and ends. The results of this inspection will be recorded and reported to the unit commanding officer. The form shown at figure 13-6 is an example of the report. Reports will be maintained by the unit security manager for one year. The Division Security Manager will be provided with a copy of this report by the 10th day of the following month. The Division Security Manager will conduct after hours security inspections for the Division Headquarters building. The Headquarters Battalion Security Manager will conduct after hours security inspections for all other headquarters areas requiring such inspections.

13005. RANDOM ENTRANCE/EXIT INSPECTION. At least once each quarter, unit security managers will conduct an unannounced random entrance/exit inspection of their unit headquarters. The purpose of the inspection is to check for unauthorized removal or introduction of classified material from/to the unit headquarters. The form shown at figure 13-7 will be used to record and report the results of the inspection to the unit commanding officer. Reports will be maintained by the unit security manager for one year. The Division Security Manager will be provided with a copy of the report by the 10th day of the month following the end of the quarter. The Division Security Manager will conduct random entrance/exit inspections for the Division Headquarters building. The Headquarters Battalion Security Manager will conduct random entrance/exit inspections for all other Headquarters Battalion areas requiring such inspections. Unit security managers will ensure that inspectors are familiar with Exhibit 13D of reference (c) prior to participating in this type of inspection.

13006. PROHIBITION AGAINST WORKING ALONE. Personnel may not work alone in communication centers, classified libraries, and areas where top secret, SCI or special access program materials are stored. Supervisors will ensure their personnel are familiar with this prohibition and will establish internal procedures to ensure compliance with this requirement.

SOP FOR IPSP

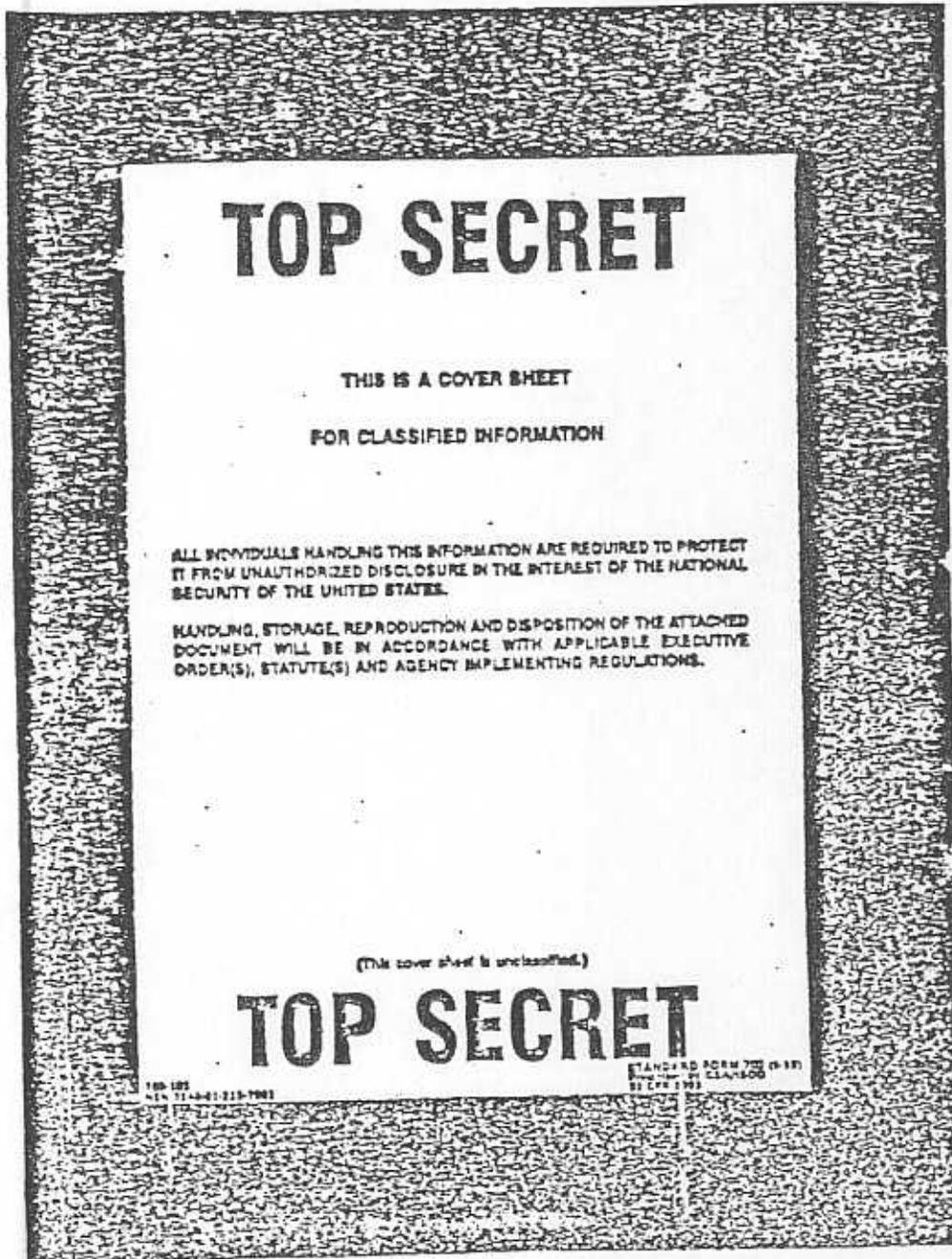


Figure 13-1. Top Secret Cover Sheet

SOP FOR IPSP

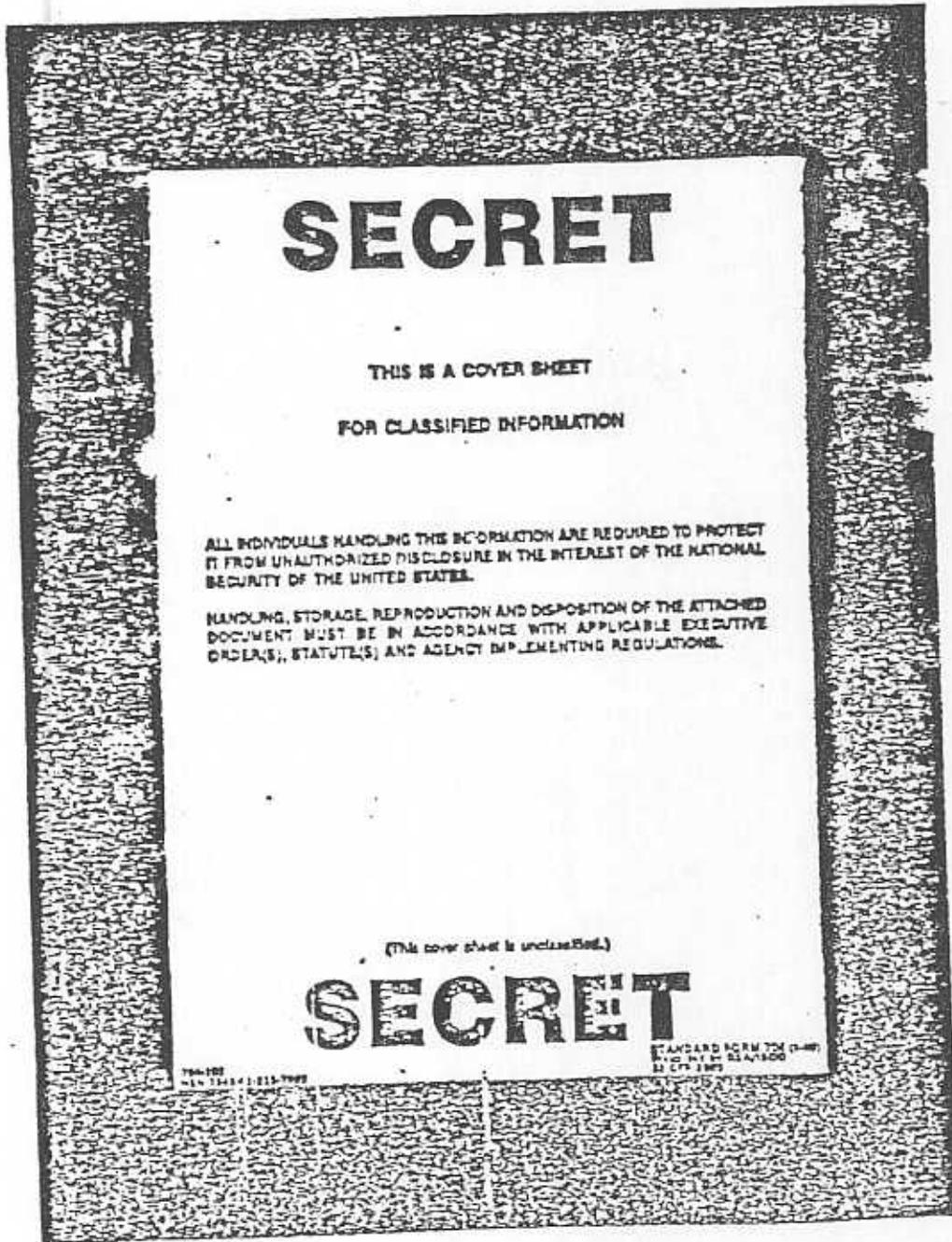


Figure 13-2. Secret Cover Sheet

SOP FOR IPSP

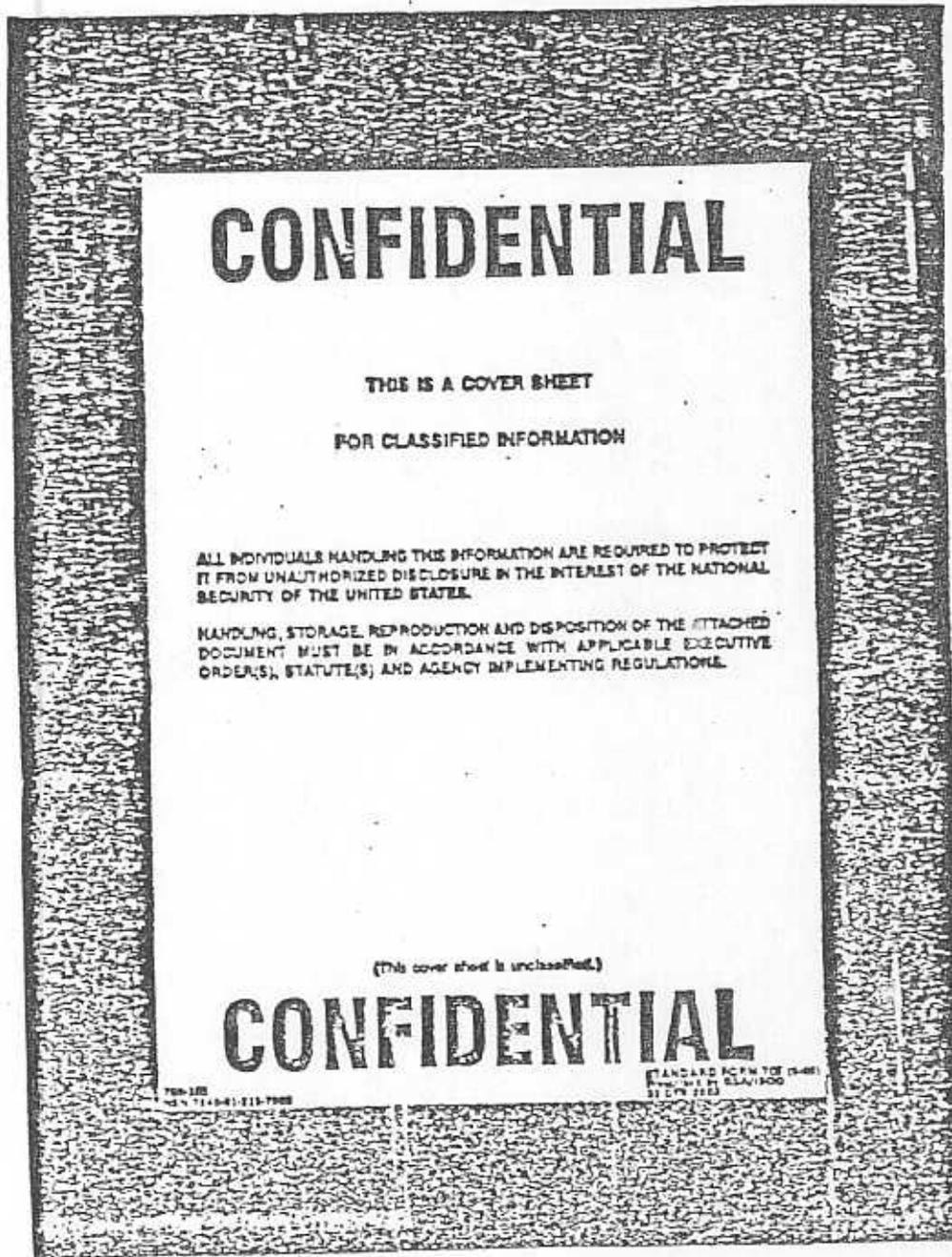


Figure 13-3. Confidential Cover Sheet

SOP FOR IPSP

SECURITY CONTAINER CHECK SHEET							
TO #				THRU #			
CERTIFICATION							
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.							
INITIALS							
1	OPENED BY	CLOSED BY		CHECKED BY		DATE CHECKED	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	DATE
1	MB	010	MB	1700	JM	1701	
2	JM	071	JM	1705	BW	1705	
3	JM	071	MB	1700	JM	1700	
4	JM	050	MB	1730	VP	1730	
5	JM	040	MB	1700	JM	1700	
SECURITY CONTAINER CHECK SHEET							
FROM #				CONTAINER #			
d JAMES				363 WOLF 13			
CERTIFICATION							
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.							
INITIALS							
JAN 8X							
1	OPENED BY	CLOSED BY		CHECKED BY		DATE CHECKED	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	DATE
STANDARD FORM NO. 64 (REV. 11-64)							
GPO : 1964 O - 253-7000							

Figure 13-4. Security Container Check Sheet

SOP FOR IPSP

ACTIVITY SECURITY CHECKLIST		BY (DDDDMMYY) (OFFICER)										ROOM NUMBER					MONTH YEAR															
		NSIC 21										363					JAN 88															
Irregularities discovered will be promptly reported to the duty room Security Office for corrective action.		(Signature) I have conducted a security inspection of this work area and checked off the items listed below.																														
FROM (if required)		THROUGH (if required)																														
ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
1. Security equipment has been tested and checked.	✓	✓	✓	✓	✓																											
2. Daily maintenance and other services and instructions are kept at prescribed standard.	✓	✓	✓	✓	✓																											
3. Windows and doors have been locked before unattended.	✓	✓	✓	✓	✓																											
4. Typewriter ribbons and ACP devices (e.g., clock, alarm) containing classified material have been removed and properly stored.	✓	✓	✓	✓	✓																											
5. Security alarms and equipment have been activated before unattended.	✓	✓	✓	✓	✓																											
BATTAL FOR DAILY REPORT	M. H. G. E. 3/3/88																															
TIME	7:25, 20, 17, 14																															

Figure 13-5. Activity Security Checklist

SOP FOR IPSP

UNIT HEADING

5500
Office Code
Date

From: Security Manager
To: Commanding Officer

Subj: UNANNOUNCED AFTER HOURS SECURITY INSPECTION

Ref: (a) OPNAVINST 5510.1H
(b) DivO 15510.9K

Encl: (1) Discrepancies

1. Per the references, an unannounced after hours security inspection was conducted on [DATE] between the hours of [TIME] and [TIME].
2. No security discrepancies were noted. (or) Discrepancies are identified in the enclosure.

SIGNATURE

Copy to:
All sections inspected
Div SecMgr

Figure 13-6. Unannounced After Hours Inspection Report

SOP FOR IPSP

UNIT HEADING

5510
Office Code
Date

From: Security Manager
To: Commanding Officer

Subj: RANDOM ENTRANCE/EXIT SECURITY INSPECTION REPORT

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. Per the references, a random entrance/exit security inspection was conducted at [UNIT], building [#], on [DATE] between [TIME] and [TIME].
2. Briefcases and similar personal belongings were inspected on entry/exit to detect unauthorized removal or introduction of classified material to this headquarters.
3. No security discrepancies were noted. (or) Discrepancies are identified in the enclosure.

SIGNATURE

Copy to:
Div SecMgr

SOP FOR IPSP

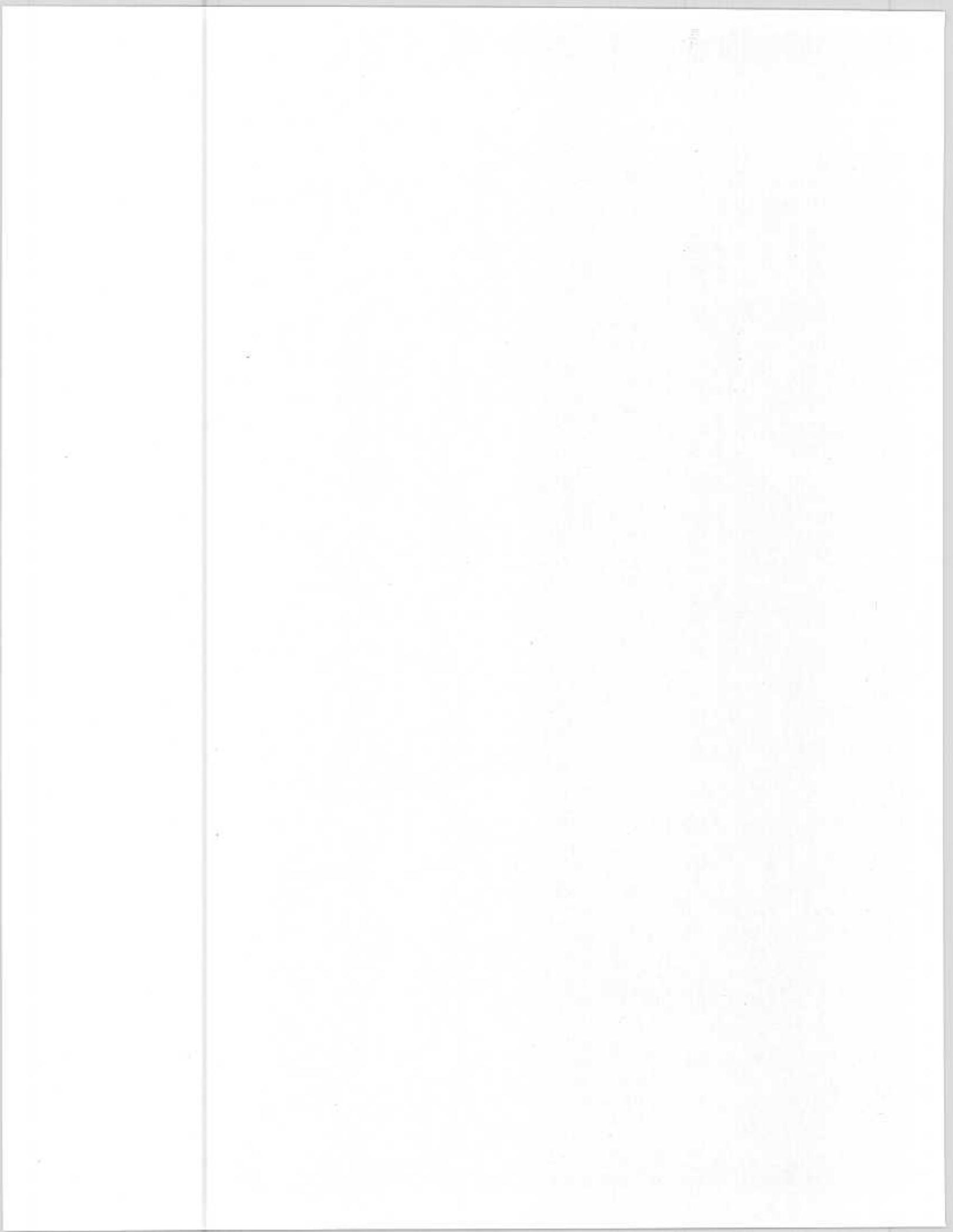
CHAPTER 14

STORAGE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	14000	14-3
STORAGE REQUIREMENTS.....	14001	14-3
VAULTS AND STRONGROOMS.....	14002	14-3
COMBINATION LOCKS, KEY OPERATED LOCKS.....	14003	14-4
SECURITY CONTAINER REPAIR.....	14004	14-4
COMBINATIONS.....	14005	14-5
SECURITY CONTAINER RECORDS.....	14006	14-6
ALARMS.....	14007	14-7

FIGURE

14-1 COMBINATION ENVELOPE STANDARD FORM 700.....		14-8
14-2 SECURITY CONTAINER RECORDS FORM OPNAV FORM 5510/12.....		14-9



SOP FOR IPSP

CHAPTER 14

STORAGE

14000. BASIC POLICY. The Commanding General and commanding officers are responsible for safeguarding all classified information within their commands. They must ensure that classified information which is neither being used nor under the personal observation of cleared persons who are authorized access, is stored as prescribed in chapter 14 of reference (c) and this Order.

14001. STORAGE REQUIREMENTS. Classified material will only be stored in GSA approved security containers and areas authorized in writing (i.e., CMCC, SCP, SCCP), that meet storage criteria established in chapter 14 of reference (c). For subordinate units of the Division, Commanding Officers will sign authorization letters for the storage of classified material. For the Division Headquarters and Headquarters Battalion, the Division Security Manager will sign authorization letters for classified material storage. Requests for authority to store classified material will be submitted to the appropriate authorization official.

1. Any weakness, deficiency or malfunction in equipment used to safeguard classified information, will be reported to the appropriate security manager immediately. For General and Special staff sections of the Division Headquarters, problems associated with security containers, vault doors or other such equipment will be reported to the Division Security Manager.

2. High value items such as weapons, money, jewels, precious metals, etc., will not be stored in the same container used for safeguarding classified material.

3. Unit Security Managers, CMCC/SCP/SCCP Custodians and supervisors will ensure that all security containers are marked for priority of destruction per chapter 14 paragraph 14-1.4 of reference (c).

4. All GSA approved security containers not used for the storage of classified material will have a placard attached to the dial drawer with the following statement: "Not used for the storage of classified material".

14002. VAULTS AND STRONGROOMS. Storage requirements for large amounts of classified material, or odd shaped or bulky material (i.e., maps, charts, overlays, equipment) can be met by constructing and utilizing vaults or strongrooms. Vaults or strongrooms utilized within the 3d Marine Division, will conform to the standards of Exhibit 14B of reference (c).

1. When odd shaped or bulky material is stored in a vault or strongroom, the Commanding Officer will ensure that the

authorization letter for that space includes the terminology "authorized for open storage of odd shaped or bulky material".

2. Vaults and strongrooms authorized for open storage will have a Physical Security Evaluation conducted every 18 months.

3. Vaults or strongrooms will not be authorized to store top secret material in "Open Storage" under any circumstances.

14003. COMBINATION LOCKS, KEY OPERATED LOCKS. Chapter 14 paragraph 14-7 of reference (c), identifies the acceptable standards for combination locks and key operated locks authorized for use in the storage of classified material within the 3d Marine Division. Electrically actuated locks may not be used as the primary means to safeguard classified material.

1. Other combination locks or key operated locks that do not meet the standards established in reference (c), will not be used for the storage of classified material within the 3d Marine Division.

2. All security containers, vaults and strongroom doors will be equipped with a top-reading changeable combination lock, which controls the locking mechanism. Front reading combination locks on security containers, vaults and strongroom doors will be replaced.

14004. SECURITY CONTAINER REPAIR. Damaged GSA approved security containers will be repaired only by qualified personnel in accordance with the provisions established in chapter 14 of reference (c). Security container lockouts will be reported promptly to the appropriate Security Manager who will, arrange for trained personnel to open the container. Units/sections will ensure that appropriately cleared personnel are present when the container is forced open to minimize the possibility of inadvertent disclosure.

1. Base/Camp Property security containers will be opened, repaired and declared unserviceable by the base locksmith. When a unit/section experiences a container lockout, contact the base locksmith at 645-7438/7439. The caller will be given a repair order work number, and told when the work may be completed. If the lockout requires immediate attention, say so when making the call (Example: an operational commitment necessitates immediate access to the material in the container).

a. If the security container is manipulated open without damage, and minor repairs or adjustments are performed, record the repairs/adjustments on the containers OPNAV Form 5510/12, see paragraph 14006.

b. If the security container is damaged during opening, but deemed repairable by the locksmith, ensure that the locksmith receipts for the container before allowing removal from the

unit/section work area.

c. If the security container is damaged and not repairable, the locksmith will prepare and issue to the unit/section Responsible Officer (RO), a Limited Technical Inspection (LTI) form, to substantiate unserviceability of the container. The LTI form will accompany paperwork necessary to survey the container through the appropriate Base/Camp Property account.

2. Table of Equipment (T/E) security containers will be opened, repaired and declared unserviceable by members of General Support Maintenance (GSM) Company, Maintenance Battalion, 3d FSSG. When a unit/section experiences a container lockout, contact GSM at 637-1306. A contact team may be dispatched to the location of the container, to open or repair the container in place. If a contact team is not available, the container may need to be transported to GSM for the necessary work.

a. The unit/section RO will ensure that a Equipment Repair Order (ERO) is opened prior to work being performed on the container by GSM personnel.

b. If the container is manipulated open without damage and minor repairs/adjustments are performed, record the repairs or adjustments on the containers OPNAV Form 5510/12, see paragraph 14006.

c. If the container is damaged during opening, but deemed repairable, ensure that GSM personnel receipt for the container before it is removed from the unit/section work area.

d. If the container is damaged during opening and deemed unrepairable, GSM personnel will close out the ERO and transport the container to Camp Kinser for disposal. The unit/section RO should get a copy of the ERO for the unit supply section to drop the container from the units T/E account.

3. In case of a lockout, the appropriate unit Security Manager will;

a. Be notified whenever a unit/section experiences a lockout.

b. Ensure that every effort has been made to open the container before it is opened by force.

c. Ensure that appropriate action is taken to protect the classified contents of the container after it has been opened.

d. Determine if negligence was the cause for the lockout.

14005. COMBINATIONS. Combinations to security containers used to store classified material will be assigned the same classification as the material stored in the container. Combinations will be

changed only by personnel having that responsibility and an appropriate security clearance.

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

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

b. The combination has been subject to possible compromise or the security container has been discovered unlocked and unattended.

c. The container (with built-in lock) or the padlock is taken out of service. Built-in combination locks will be reset to the standard combination 50-25-50. Combination padlocks will be reset to the standard combination 10-20-30.

2. Security containers used to store NATO classified material will have their combinations changed at least every six months, or on the occasions identified in paragraph 14005.1 above.

3. Before security containers are placed in storage, the standard combination identified in paragraph 14005.1 above will be set on the container. If personnel are not available to set the standard combination on the container; the containers combination will be attached to the outside of the dial drawer and the containers dial drawer will be locked in the open position.

4. Record each classified material container combination and dialing instructions for the container, using Standard Form 700, figure 14-1. List the custodian, and each person authorized access to the combinations, on the envelope.

5. Each CMCC, SCP or SCCP will designate one container as a "Master Container". Within the Division, security containers will be marked with painted numbers; e.g. CMCC 1, 2, 3, SCP 1, 2, 3, SCCP 1, 2, 3. Container #1 will always be the master container. The master container will always hold the combinations to all other containers within that section; e.g. CMCC, SCP, SCCP. The combination of an SCCPs master container will be held by the parent SCP. The combination(s) of an SCP(s) master container will be held by the unit CMCC. Division CMCC will store its combination for the outer and inner vault doors and master container with the 1st Special Security Communications Team (SSCT) located on the second floor of building 4211. Combinations of vault doors and master containers of subordinate unit CMCCs will be stored at the Division CMCC.

14006. SECURITY CONTAINER RECORDS. Security Managers will ensure that a Security Container Records Form (OPNAV Form 5510/12), Figure 14-2, is maintained for all GSA approved security con-

tainers, whether used for the storage of classified material or not. Security Managers and/or custodians will ensure all GSA approved security containers are inspected annually. Deficiencies identified during annual inspections will be reported to the unit Security Manager. Requests for repairs will be accomplished per paragraph 14004 of this chapter. Repairs will be recorded on the form in accordance with instructions contained in chapter 14 of reference (c). When a form is completely filled in, a new form will be prepared for the container. All forms will be maintained and transferred with the container when taken out of service and returned to the supply system.

14007. INTRUSION DETECTION SYSTEMS. Refer to chapter 14 of reference (c) for criteria related to intrusion detection systems, intended for use in protecting classified material within the environs of the 3d Marine Division.

SOP FOR IPSP

CLASSIFICATION			
SECURITY CONTAINER INFORMATION 1. COMPLETE PART 1 AND PART 2 ON SIDE OF FLAP. 2. AS WITH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. INSERT PARTS 1 AND 2 INTO THE SECURITY CLASSIFICATION STORAGE IN THE CONTAINER. 4. ATTACH PART 3 AND INSERT IN ENVELOPE. 5. SEAL ENVELOPE AND ATTACH TO INSIDE OF CONTAINER.	1. AREA OR POINT OF ORIGIN	2. DATE DATE OF ORIGIN	3. CODE NO.
		WOLF	363
	4. ACTIVITY APPROVAL, SYMBOL, AND TYPE OF OFFICE		5. DATE DATE OF
	NSIC-23		13
	6. NAME & TYPE OF OFFICE	7. DATE & TIME LAST	8. DATE COMPLETION
	TRT Moral	8 6 0	13 Sep 87
	9. NAME AND SIGNATURE OF PLACED OFFICE OFFICER		
	John Doe		
10. INFORMATION WITH ONE OF THE FOLLOWING INITIALS, IF THE OFFICER IS FOUND DEAD AND UNRECOVERED			
11. EMPLOYEE NAME	12. HOME ADDRESS	13. PHONE NUMBER	
JOHN DOE	8673 Georgia Ave	Willow Spring (301) 427-9520	
B. JOE SMITH	1224 Oak Hill Rd. Clary	(301) 952-1724	
1. ATTACH TO INSIDE OF CONTAINER			
CLASSIFICATION			

CLASSIFICATION	
Container Number	
13	
CONTAINER	
1	1
2	2
3	3
4	4
REMARKS	
THE COPY CONTAINING CLASSIFIED INFORMATION MUST COMPLY WITH THE FOLLOWING REQUIREMENTS	
CLASSIFICATION	

Figure 14-1. Combination Envelope Standard Form 700

SOP FOR IPSP

SECURITY CONTAINER RECORDS FORM
OPNAV FORM 5510/12 (10-79)

CONTAINER NUMBER 0294	LOCATION Room 780 CNS	OFFICE CODE CMO (07-XXX)	TYPE OF CONTAINER Mosler/S drawer legal
DATE INSPECTED (Date)	CLASS OF CONTAINER <input type="checkbox"/> Class 1 <input type="checkbox"/> Class 2 <input type="checkbox"/> Class 3 <input type="checkbox"/> Class 4 <input checked="" type="checkbox"/> Class 5		FEDERAL STOCK NUMBER 7110-91-9193
STOCK NUMBER 16133	DATE OF MANUFACTURE (Date)	QUANTITY OF ELEMENTS 10 linear feet	CLASSIFICATION Confidential - Secret
WEIGHT CLASS AND WEIGHT	WEIGHT CLASS AND WEIGHT	WEIGHT CLASS AND WEIGHT	

PERCENTAGE OF ELEMENTS IN EACH WEIGHT

WEIGHT 0 a WEIGHT 65 a WEIGHT 25 a WEIGHT 0 a

TYPE OF LOCK MECHANISM Mosler Handchange	TYPE Hand	DATE OF MANUFACTURE (Date)
--	---------------------	--------------------------------------

CONDITION OF CONTAINER
Good

REMARKS
See reverse

OPNAV FORM 5510/12 (10-79) (CONT)

INSPECTION AND REPAIRS			
DATE INSPECTED	INSPECTED BY	CONDITION	REPAIRS MADE/DEFERRED
(Date)	abc	NEW	
(Date)	bcw	LOCKOUT	Drawer lead replaced (Date)

Figure 14-2. Security Container Records Form OPNAV Form 5510/12

SOP FOR IPSP

CHAPTER 15

TRANSMISSION OF CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	15000	15-3
TRANSMISSION OF CLASSIFIED MATERIAL VIA THE U. S. POSTAL SYSTEM.....	15001	15-3
TRANSMISSION OF CLASSIFIED MATERIAL VIA SECURE FACSIMILE.....	15002	15-3
TRANSMISSION OF CLASSIFIED MATERIAL OUTSIDE THE U. S. DEPARTMENT OF DEFENSE.....	15003	15-5

FIGURE

15-1 RECORD OF RECEIPT.....		15-6
-----------------------------	--	------

SOP FOR IPSP

CHAPTER 15

TRANSMISSION OF CLASSIFIED MATERIAL

15000. BASIC POLICY. All members of the 3d Marine Division will strictly adhere to the procedures and restrictions for the transmission of classified material promulgated in chapter 15 of reference (c), this Order and other appropriate directives.

1. Classified information will be transmitted either in the custody of an appropriately cleared individual or by an approved system or carrier, and in accordance with the provisions of reference (c), this Order and other appropriate directives.
2. Transmission includes any movement of classified information or material from one place to another, regardless of the means of transportation, i.e., mail, courier, courier service, or electrical means (including secure facsimile).
3. All classified material to be transmitted to another unit/section within the Division will be sent via appropriate communications facilities and/or CMCC channels with the exception of SCI material.
4. Classified material to be mailed to organizations or activities outside the Division will be mailed per the provisions of chapter 15 of reference (c) and paragraph 15001 of this Order.

15001. TRANSMISSION OF CLASSIFIED MATERIAL VIA THE U. S. POSTAL SYSTEM. Per the provisions contained in chapter 15 of reference (c), some (excluding top secret) classified material may be transmitted via the U.S. Postal System. Within the 3d Marine Division, the following procedures will be adhered to:

1. Only unit CMCC personnel will process classified material for transmission via the U.S. Postal System.
2. Packaging will be prepared by the section with custodial responsibility of the classified material.
3. The material and packaging (unsealed) will be delivered to the appropriate CMCC for accounting, preparation of appropriate receipt(s) shown in figure 15-1, sealing and transport to the appropriate U.S. Postal facility.
4. Per the provisions of reference (c), classified material will be sent via registered U.S. mail only.

15002. TRANSMISSION OF CLASSIFIED MATERIAL VIA SECURE FACSIMILE. Classified material may be transmitted via secure facsimile under the following restrictions and procedures.

1. Top secret material may not be transmitted via secure facsimile.
2. Secret material may be transmitted via secure facsimile using the following procedures.
 - a. The unit has access to a secure facsimile machine approved for the transmission of secret material.
 - b. The secret material is controlled by the unit CMCC in accordance with the instructions contained in this Order.
 - c. CMCC personnel will ensure that appropriate classification markings appear on each page of the material.
 - d. CMCC personnel will ensure that there are no restrictions associated with the material being sent to the receiving unit (i.e., dissemination restrictions, activity outside the Department of Defense).
 - e. The last page of the transmitted material will be a reproduced receipt form (see figure 15-1), containing the following information.
 - (1) Complete identification of the material transmitted, including the CMCC control number and total number of pages in the package (including receipt form page).
 - (2) Complete mailing address of the sending unit CMCC.
 - (3) Instructions that the material and receipt be delivered to the receiving unit CMCC for control and return of the receipt form to the sending CMCC.
 - (4) Name of the individual, section or unit the material is intended for.
 - f. CMCC personnel will transmit the material or deliver the material for transmission to the facility with secure facsimile capability.
 - g. The sending unit CMCC will retain the transmitted material, the unsigned receipt form and the facsimile generated receipt in a suspense file until a signed receipt is received from the receiving unit CMCC.
 - h. After 30 days, if a signed receipt is not received from the receiving unit CMCC, a copy of the receipt in the suspense file will be forwarded to the receiving unit CMCC with a request for tracer action.
3. Confidential material may be transmitted via secure facsimile using the following procedures.

a. The unit has access to a secure facsimile machine approved for the transmission of confidential material.

b. CMCC personnel will ensure that appropriate classification markings appear on each page of the material.

c. CMCC personnel will ensure that there are no restrictions associated with the material being sent to the receiving unit, (i.e., dissemination restrictions, activity outside the Department of Defense).

d. The last page of the transmitted material will contain the following information.

(1) Complete identification of the material transmitted and total number of pages.

(2) Complete mailing address of the sending unit CMCC.

(3) Name of the individual, section or unit the material is intended for.

e. The sending unit CMCC will retain the transmitted material and the facsimile generated receipt in a suspense file for 30 days, and then destroy the material.

15003. TRANSMISSION OF CLASSIFIED MATERIAL OUTSIDE THE U.S. DEPARTMENT OF DEFENSE. Members of the 3d Marine Division are not authorized to transmit classified material to individuals, or organizations outside the U.S. Department of Defense. Members of the 3d Marine Division are not authorized to transmit or release classified material to foreign nationals or foreign governments unless authorized in accordance with the provisions and restrictions promulgated by reference (c) and other applicable directives.

SOP FOR IPSP

FORM 10-1 (REV. 1-68) DA FORM 10-1 (11)		RECORD OF RECEIPT REFERENCE REQUEST FILE				THIS RECEIPT MUST BE SIGNED AND RETURNED
ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF RECEIPT	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF COPIES TO BE RETURNED	REGISTERED FLAGGED
Op-XXX	812345	(Date)	Security Classification Guide	1	1	
<small>APPROPRIATE AGENCY RECEIVING OR RETURNING</small> CNO Op-XXX31				<small>DATE</small> (Date)		

Figure 15-1. Record of Receipt

SOP FOR IPSP

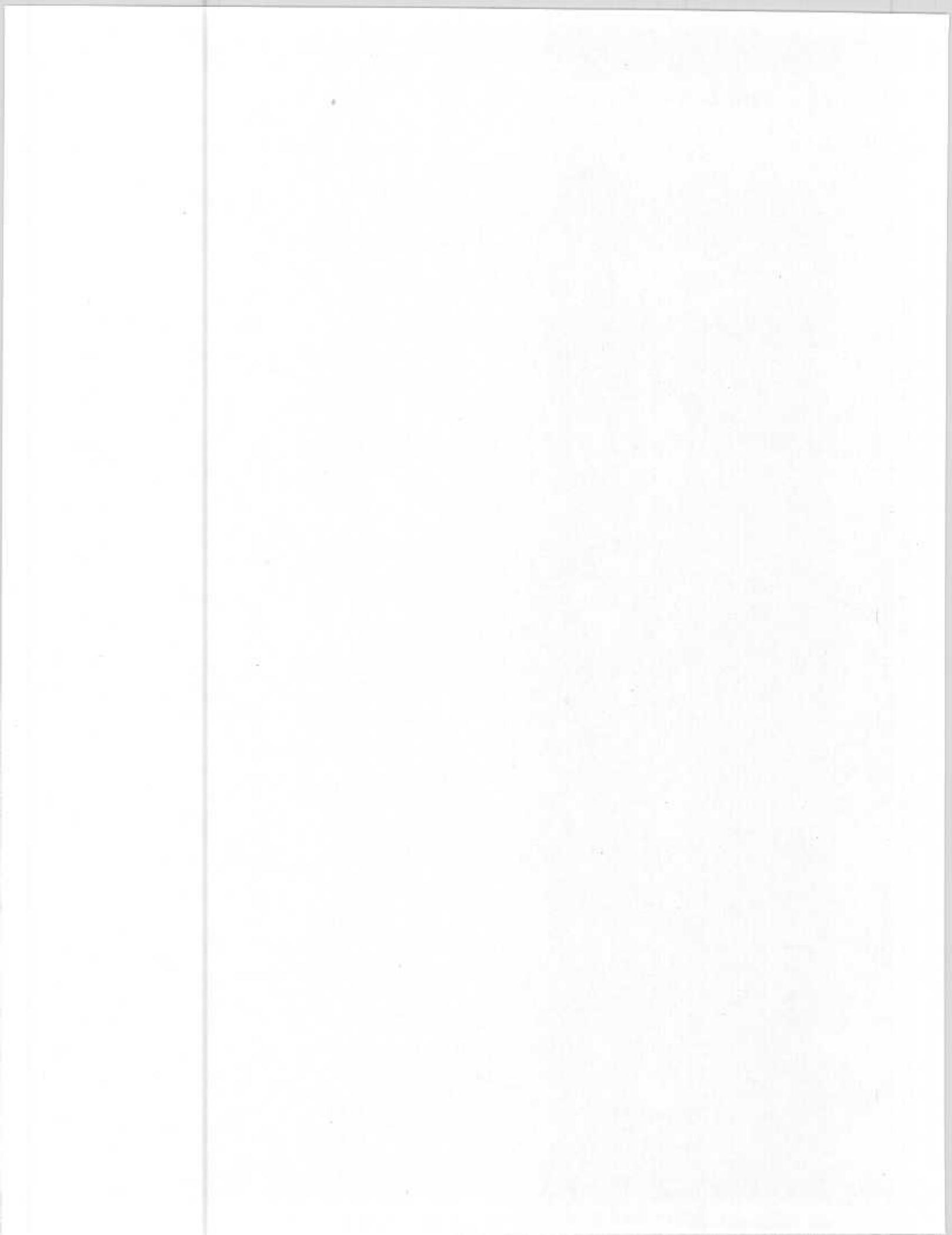
CHAPTER 16

HAND CARRYING CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	16000	16-3
HAND CARRYING WITHIN A HEADQUARTERS.....	16001	16-3
HAND CARRYING ON ISLAND.....	16002	16-3
HAND CARRYING OFF ISLAND.....	16003	16-3
HAND CARRYING ABOARD COMMERCIAL AIRCRAFT....	16004	16-5
HAND CARRYING ON RETURN TRIP.....	16005	16-5
COURIER CARDS.....	16006	16-5

FIGURE

16-1	SAMPLE AUTHORIZATION LETTER FOR HAND CARRYING CLASSIFIED MATERIAL OFF ISLAND.....	16-7
16-2	SAMPLE BILINGUAL STATEMENT FOR USE IN JAPAN AND OKINAWA.....	16-10
16-3	SAMPLE BILINGUAL STATEMENT FOR USE IN THE REPUBLIC OF KOREA.....	16-11



SOP FOR IPSP

CHAPTER 16

HAND CARRYING CLASSIFIED MATERIAL

16000. BASIC POLICY. Every precaution must be taken to prevent unauthorized disclosure when individuals are hand carrying classified material within a headquarters in the pursuit of daily duties, outside the headquarters on island to another command, or off island in a travel status.

16001. HAND CARRYING WITHIN A HEADQUARTERS. When classified material is being carried within a headquarters from office to office, it will be carried using an appropriately marked cover sheet or file folder to protect against casual observation. Classified material will not be carried into public areas such as barber shops, PXs, commissaries, etc.

16002. HAND CARRYING ON ISLAND. Classified material may be hand carried between headquarters on island under the following conditions.

1. An individual/courier hand carrying classified material must have the appropriate clearance and access for the material being carried.
2. The individual/courier must have been issued and have in their possession a DD Form 2501 (Universal Courier Authorization Card). A courier card is not required if the courier is transporting the classified material to an adjacent building.
3. The material being transported must not be readily available at the intended destination.
4. The material must be wrapped per paragraph 16-2 of reference (c) and enclosed in either a locked briefcase or sealed courier pouch. This requirement applies to classified material carried from one building to another.
5. The individual/courier must maintain constant positive control over the material during transit. On base, classified material will not be transported by bicycle or motor cycle. Classified material being hand carried to another unit that requires leaving a U. S. Government installation, will be transported in a government vehicle unless authorized by the appropriate unit security manager.

16003. HAND CARRYING OFF ISLAND. Hand carrying classified material off island by personnel in a travel status, utilizing government conveyance, will not be authorized unless it is absolutely necessary to accomplish operational objectives.

1. When it is determined that such requirements exist, a request for authorization to carry classified material off island will be submitted to the cognizant security manager (i.e., Division Security Manager for Division Headquarters personnel, appropriate unit security manager for all others). The request will contain the following information:

- a. Full name, grade and service number of traveler.
- b. Traveler's Armed Forces identification card number.
- c. Description of material being carried (generic, i.e., 14 secret brief slides, secret proposed OPORD, etc.).
- d. Point of departure.
- e. Carrier airline and flight itinerary.
- f. Destination (Command and complete mailing address)
- g. Known transfer points.
- h. Date required.
- i. DD 2501 serial number.
- j. Justification/Justification for return hand carry (Reason why other authorized means of transmission is not used).
- k. Point of contact and telephone number.

2. The unit security manager will prepare an authorization letter to hand carry classified material using the format shown in figure 16-1. The letter will include a signed endorsement by the intended courier that he or she has read and understands the provisions contained in the letter and chapter 16 of reference (c). The letter will be retained by the Division Security Manager for Division Headquarters personnel or the appropriate unit security manager for other personnel, for a period of two years.

a. Requests for travel orders to the adjutant will identify courier requirements and clearance status. A copy of the travel orders will be provided to the appropriate unit security manager.

b. Prior to departure, but in sufficient time to permit required actions, the individual hand carrying the material will deliver the material, an inventory of the material and addressed wrapping material to the appropriate CMCC. CMCC personnel will verify the material against the inventory and, if correct, will maintain a copy of the inventory for action per subparagraph (c) below. CMCC personnel will then prepare the material for hand carrying using the wrapping materials provided.

c. Upon return of the material to the command, the individual will turn the material into the appropriate CMCC. CMCC personnel will check the material against the inventory and report any discrepancies to the appropriate unit security manager. If there are no discrepancies, the material will be returned to the appropriate control point (CMCC, SCP, SCCP) for storage.

16004. HAND CARRYING ABOARD COMMERCIAL AIRCRAFT. The transporting of classified material aboard commercial passenger aircraft outside the continental limits of the United States is prohibited without the written consent of the Commanding General, Marine Forces Pacific (COMMARFORPAC). Requests for authorization to hand carry classified material aboard commercial aircraft will be directed to the Division Security Manager at least 25 working days prior to departure date. The request will contain the information required in paragraph 16003. If the request is approved by the Division Security Manager, the request will be forward to COMMARFORPAC via message with an information copy forwarded to the requesting unit. When approval is received from COMMARFORPAC, the message will be considered as an endorsement to the travel orders. A courier authorization letter will be prepared per the detailed instructions contained in chapter 16, paragraph 16-8 of reference (c). A copy of the letter will be maintained by the unit security manager for two years. Hand carrying classified material aboard foreign flag carriers is prohibited.

16005. HAND CARRYING ON RETURN TRIP. The appropriate unit security manager must be made aware of any requirements to hand carry classified material aboard commercial aircraft on the return leg of travel. The courier authorization letter issued by the security manager will have an expiration date of seven days from date of issue. If justified by the supervisor in his request, the unit security manager will make provisions for the visited command to revalidate the courier authorization letter.

16006. COURIER CARDS. The Universal Courier Authorization Card, DD Form 2501 supersedes all other command developed courier authorizations except for NAVINTCOM 5510-69 (Rev9-86), Sensitive Compartmented Information (SCI) Courier Card. DD Form 2501s are serialized and must be controlled and accounted for. Commanding officers, security managers or assistant security managers (if assigned), are authorized to issue the DD Form 2501, Universal Courier Authorization Card. The 3d Marine Division Special Security Office is responsible for procuring, controlling, accounting for and issuing SCI courier cards.

1. A written request for issue of DD Form 2501 courier card will be submitted to the commanding officer. For members of General and Special staff sections of the Division Headquarters, requests will be submitted to the Commanding Officer, Headquarters Battalion.

a. Issuing officials will:

(1) Ensure that the individual has been granted appropriate clearance and access before issuing a courier card.

→ (2) Ensure only personnel assigned duties in CMS, CMCC and top secret control positions are authorized to courier top secret material. All other courier authorizations will be limited to secret or confidential, based on individual's clearance and access granted by the command.

(3) Maintain a record by serial number of cards on hand, issued, turned in and destroyed, and signatures of authorized couriers to whom cards have been issued.

(4) Affix a bilingual statement (figure 16-2 for Japan and Okinawa), to each DD Form 2501 issued. Figure 16-3 is a bilingual statement for use in the Republic of Korea.

(5) Ensure authorized couriers understand and comply with the requirements of references (c), (v), (w) and this Order.

(6) Ensure authorized couriers understand that possession of DD Form 2501 does not constitute authorization to courier classified material off island. See paragraph 16003 and 16004 of this Order.

(7) Establish expiration dates for DD Form 2501 not to exceed one year from date of issue. New cards may be reissued for one year to those personnel who have a continued courier requirement.

(8) Destroy turned in cards and annotate records accordingly.

(9) Establish administrative procedures that ensure DD Form 2501 courier cards are returned prior to an individuals transfer.

b. Authorized couriers will:

(1) Ensure proper control and security of the card while in their possession.

(2) Immediately report the loss or theft of the card to the issuing official with a statement identifying events surrounding the loss or theft. Issuing officials will determine if other investigative agencies need to be notified.

(3) Turn in the card to the issuing official when they are relieved from courier duty, when the card is mutilated or upon transfer.

SOP FOR IPSP

HEADING

5511
ID SYMBOL
(Date)

From: Security Manager, (unit)
To: (Individual authorized to hand carry classified material)
Subj: AUTHORIZATION TO HAND CARRY CLASSIFIED MATERIAL OFF ISLAND
ABOARD U.S. GOVERNMENT OWNED OR CONTROLLED AIRCRAFT
Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9K

1. You have been authorized to hand carry classified material off island while in an official travel status.

2. The following instructions for hand carrying classified material apply:

a. Whenever classified information is hand carried on military or commercial aircraft, it shall be enclosed in two opaque sealed envelopes or similar wrappings where size permits. The wrappings shall conceal all classified characteristics. The sealed outer envelope, package or carton containing classified material shall be signed on its face by the official who signed the letter of authorization to hand carry classified material, and addressed as if it were to be mailed to this command.

b. The persons carrying classified information should process through the airline ticketing and boarding procedure in the same manner as all other passengers except for the following:

(1) The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes. Such envelopes should be contained in a briefcase or other carryon luggage. The briefcase or luggage shall be routinely offered for inspection for weapons and such. The screening officials may check the envelope by X-ray machine, flexing, feel, weight, etc., without opening the envelopes themselves.

(2) Opening or reading of the classified documents by the screening official is not permitted.

(3) Should you at any time encounter difficulty with customs, you are to follow the procedures outlined in your courier authorization letter.

Figure 16-1. Sample Authorization Letter For Hand Carrying Classified Material Off Island

SOP FOR IPSP

HEADING

5511
(CODE)
(DATE)

FIRST ENDORSEMENT on _____

From: (Individual authorized to hand carry classified material)
To: Security Manager, (Unit)

Subj: AUTHORIZATION TO HAND CARRY CLASSIFIED MATERIAL OFF ISLAND
ABOARD U. S. GOVERNMENT OWNED OR CONTROLLED AIRCRAFT

1. I have read and understand the instructions pertaining to the handling of classified material in my custody while I am in a travel status. I understand that authorization to hand carry classified material off the island of Okinawa is:

a. Limited to travel aboard U.S. Government aircraft or other means controlled by the U.S. Government.

b. That transportation of classified material aboard a commercial aircraft without prior written approval of COMMARFORPAC is prohibited.

2. I further understand that the classified material I am carrying will be inventoried by (unit) Classified Material Control Center prior to my departure and upon my return. Also, any classified material acquired by me will be turned into (unit) Classified Material Control Center upon my return in order that it may be placed under proper control.

SIGNATURE

SOP FOR IPSP

THE BEARER OF THIS IDENTIFICATION IS ON OFFICIAL BUSINESS AND IS CHARGED WITH THE CUSTODY OF OFFICIAL CLASSIFIED DOCUMENTS OR MATERIAL.

NO RESTRICTION WHATEVER WILL BE PLACED UPON HIS PERSON OTHER THAN THAT NECESSARY TO ASCERTAIN HIS NAME AND ORGANIZATION. DOCUMENTS AND/OR MATERIAL IN HIS POSSESSION WILL NOT BE REMOVED FROM HIS POSSESSION NOR OPENED, NOR INSPECTED.

この身分証明書は公署に従事しており、公の職務又は
又は資料の保持の責に任しているものである。この者はその氏名
及び所属を証明する以上、如何なる目的のためにも
その所持する文書又は資料は其の所持する文書又は資料
がその所持する文書又は資料を其の所持する文書又は資料

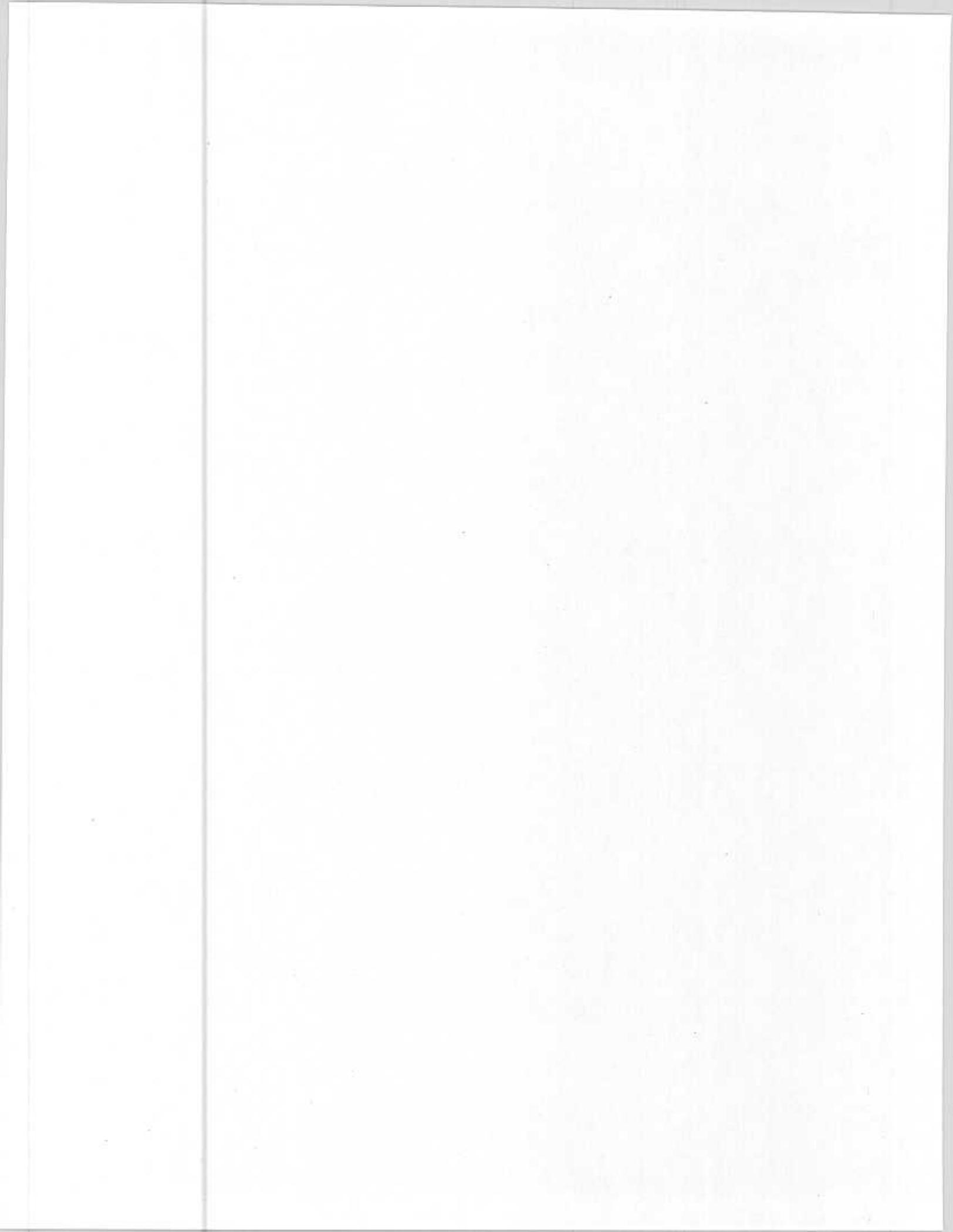
Figure 16-2. Sample Bilingual Statement For Use In Japan And Okinawa

SOP FOR IPSP

THE BLANKS OF THIS IDENTIFICATION CARD IS A U. S. MARKING BY OFFICIAL BUSINESS
AND IS CHANGED WITH THE CUSTOM OF OFFICIAL CLASSIFIED INFORMATION ON SEPARATE
NO RESTRICTION WHATSOEVER WILL BE PLACED UPON THE PERIOD OTHER THAN THAT INDICATED
BY ACTUALLY THE MARK AND ORGANIZATION. DOCUMENTS AND FOR OFFICIAL IN HIS PRE-
SENCE WILL NOT BE REMOVED FROM HIS PRESENCE, FOR OFFICE AND INSPECTOR.

이서명어 미국방역자 특별서명 취업자이다.
이서명어 상영로오우우우우를 확인 하는것외에
언해하지마시오. 이서명어 오쪽 특별 서명
적기 하지마오 보지 마시오.

Figure 16-3. Sample Bilingual Statement For Use In The Republic Of Korea

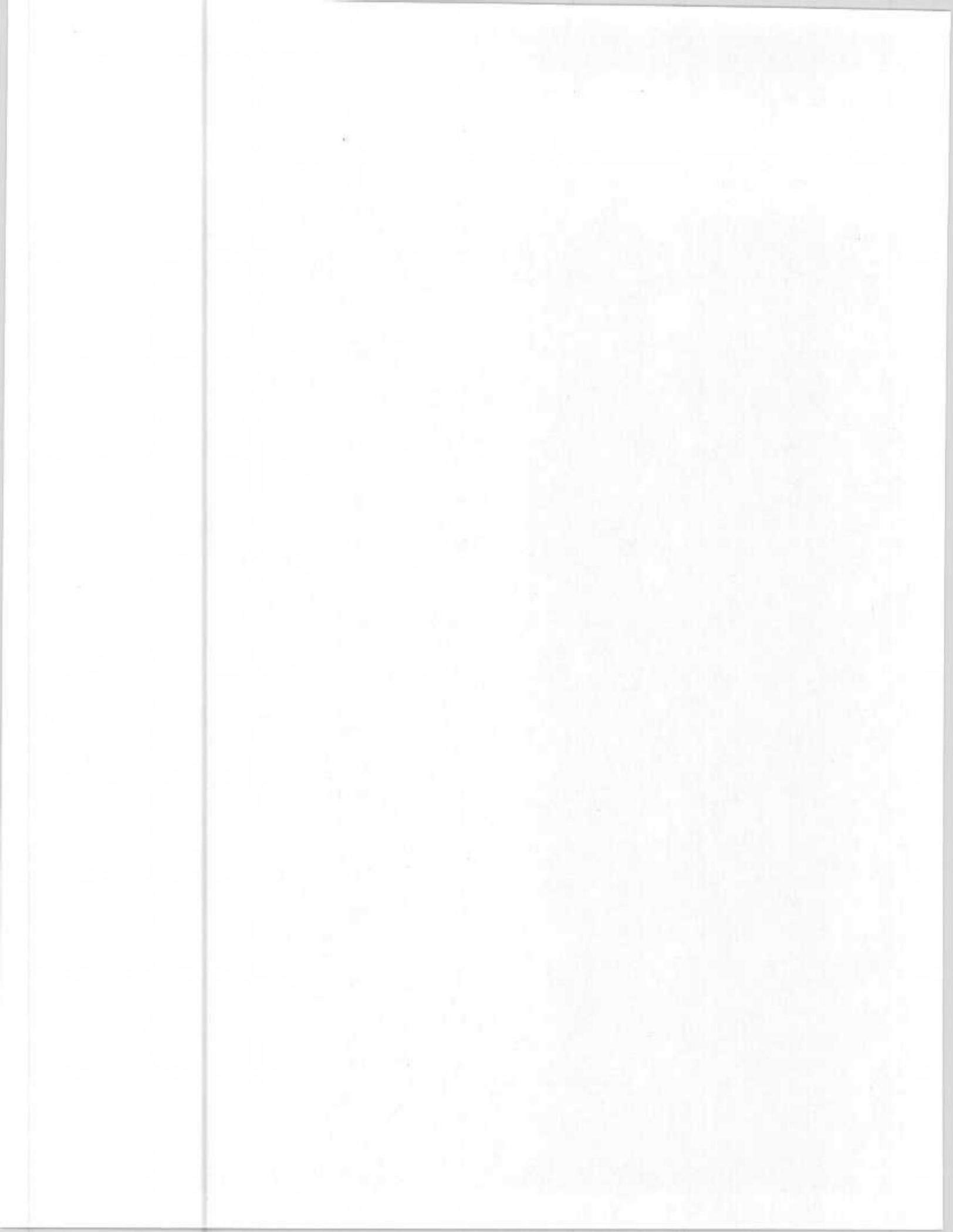


SOP FOR IPSP

CHAPTER 17

DESTRUCTION OF CLASSIFIED AND UNCLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	17000	17-3
DESTRUCTION PROCEDURES.....	17001	17-3
DESTRUCTION OF SECRET MESSAGES.....	17002	17-4
METHODS OF DESTRUCTION OF DESTRUCTION FOR CLASSIFIED MATERIAL.....	17003	17-4
DESTRUCTION OF UNCLASSIFIED MATERIAL.....	17004	17-4
DESTRUCTION OF CLASSIFIED MICROFICHE.....	17005	17-4
DECLASSIFYING ADP STORAGE MEDIA.....	17006	17-4
EMERGENCY DESTRUCTION.....	17007	17-5
FIGURE		
17-1 CLASSIFIED MATERIAL DESTRUCTION REPORT (OPNAV FORM 5511/12).....		17-6



SOP FOR IPSP

CHAPTER 17

DESTRUCTION OF CLASSIFIED AND UNCLASSIFIED MATERIAL

17000. BASIC POLICY. Within the 3d Marine Division, classified material will be destroyed per the instructions contained in chapter 17 of reference (c) and this Order.

1. Classified record material may be destroyed only when destruction is the disposition authorized by the current edition of SECNAVINST 5212.5, the instruction governing disposal of Navy and Marine Corps records.
2. All other classified material will be destroyed as soon as it is no longer required and will not be retained for more than five years from the date of origin unless authorized by the current edition of SECNAVINST 5212.5. Each unit/section of the 3d Marine Division will establish an annual classified records "clean out" day during which a portion of the work will be devoted to destruction of unneeded classified holdings. Units/sections may elect to schedule their "clean out" day to coincide with the annual review of classified holdings which is conducted no later than 15 February of each year.
3. Specific requirements for the destruction of COMSEC material can be found in references (d) and (e).

17001. DESTRUCTION PROCEDURES. Classified material will be destroyed only by authorized means. Personnel actually involved in the destruction process will have the appropriate security clearance and be granted access to the same level of the material being destroyed.

1. The destruction of top secret and secret material will be recorded. Destruction may be recorded on OPNAV Form 5511/12 (Classified Material Destruction Report) shown in figure 17-1. Reproduced OPNAV Form 5511/12 or other locally produced destruction reports that include all the information required on OPNAV Form 5511/12 may be used to record the destruction of top secret and secret material.
2. Two officials will be responsible for destroying top secret and secret material and will sign the record of destruction.
3. Within the 3d Marine Division, only the Commanding General, commanding officers, or top secret control officers may authorize the destruction of top secret material.
4. The OIC, CMCC and SCP custodians may authorize the destruction of secret material. If secret material is destroyed by SCP personnel, the original destruction report will be submitted to the unit CMCC and a copy will be maintained in SCP destruction files.

5. All destruction reports for top secret and secret material, will be maintained for a minimum of two years from the actual date of destruction.

6. Confidential material (documents, messages) and classified waste (reproduction overruns, rough drafts, etc.) will be destroyed by authorized means by appropriately cleared personnel, but do not require a record of destruction.

17002. DESTRUCTION OF SECRET MESSAGES. Effective 31 December 1991, the requirement for recording the destruction of secret message traffic was rescinded, with some exceptions.

1. Recording the destruction of secret messages received through supporting communications facilities, with the exception of Special Access Program and NATO information is no longer required, if the messages are destroyed by two properly cleared personnel.

2. The destruction of secret messages must be recorded on OPNAV Form 5511/12 if the destruction is accomplished by only one properly cleared person.

3. Secret messages received via registered mail, courier, or secure facsimile will be controlled by unit CMCCs (see chapter 10 of this Order), destruction will be recorded on OPNAV Form 5511/12 and witnessed by two properly cleared personnel.

4. Secret messages (except for Special Access and NATO information) previously received via supporting communications facilities may be removed from unit CMCC control logs.

17003. METHODS OF DESTRUCTION FOR CLASSIFIED MATERIAL. The only authorized methods of destroying classified material for units of the 3d Marine Division, are those outlined in chapter 17 of reference (c).

17004. DESTRUCTION OF UNCLASSIFIED MATERIAL. No written/printed material within the 3d Marine Division will be discarded in trash cans. Trash cans are to be utilized for trash, (i.e., candy wrappers, soda cans, etc.). All unclassified material will be added to unit/section classified material burn bags and destroyed by burning, or destroyed by other means such as strip shredding. If units/sections elect to strip shred unclassified material, strip shredders will produce residue no wider than 1/4".

17005. DESTRUCTION OF CLASSIFIED MICROFICHE. Classified material contained or stored on microfiche will be destroyed by burning.

17006. DECLASSIFYING ADP STORAGE MEDIA

1. Destruction of ADP storage media is not always necessary. ADP storage media can be declassified and used for unclassified processing by following the instructions contained in Chapter 17,

paragraph 17-4 of reference (c). The unit ISSO should be contacted for assistance in this area.

2. Removeable hard drives (AN/UYK 83/85) used for the storage and processing of classified information, pose a special problem for the unit ISSO when the media crashes or will not allow software to overwrite the classified information. The unit ISSO will declassify the inoperative hard drive using a magnet with a field strength of at least 1500 oersted. If such a magnet is not available, the hard drive will be forwarded to the appropriate U.S. Government repair facility via CMCC channels. An Equipment Repair Order (ERO) will be opened on the defective hard drive, and accompany the hard drive to the repair facility.

17007. EMERGENCY DESTRUCTION. All units/sections of the 3d Marine Division, that hold classified material will prepare an Emergency Destruction Plan (EAP) in accordance with chapter 17, paragraph 17-7 of reference (c) and paragraph 2018 of this Order.

1. Commanding officers/security managers will ensure that the unit/section EAP is tested at least annually. Results of the test will be recorded and maintained by unit security managers and CMCC custodians for at least two years.

2. Commanding officers/security managers will ensure that the unit EAP adequately addresses the additional emergency destruction policy and guidance for COMSEC material, which can be found in references (d) and (e).

SOP FOR IPSP

CLASSIFIED MATERIAL DESTRUCTION REPORT OPNAV FORM 5511/12 REV. 8-78 (41) 5010-108-0100		CLASSIFICATION (Indicate when this or other classification is changed) UNCLASSIFIED				
TO: Commanding Officer, USS NEVERSAIL <small>(Name, phone, and address of activity)</small> Top Secret Control Officer						
<small>The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation, OPNAV INSTRUCTION 5010.10</small>			<small>The purpose of this form is to provide activities with a record of destruction of classified material. Also, reports may be utilized for reports to activities regarding the work, where such reports are necessary.</small>			
DESCRIPTION OF MATERIAL						
SIGNATURE	DESCRIPTION	DATE	COPY NO.	CLASS. AUTHORITY	TOTAL NO. COPIES	
80052	CINCPACFLT letter	(Date)	1	4	4	
<small>OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION (Signature, Last, First, Middle)</small> _____			<small>DATE OF DESTRUCTION</small> _____ (Date)			
<small>OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION (Signature, Last, First, Middle)</small> John Doe			<small>OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION (Signature, Last, First, Middle)</small> Jane Smith			

Figure 17-1. Classified Material Destruction Report (OPNAV Form 5511/12)

SOP FOR IPSP
CHAPTER 18
VISITOR CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	18000	18-3
GENERAL VISITING.....	18001	18-4
CONTROL MEASURES.....	18002	18-4
CLASSIFIED VISITS TO DEPARTMENT OF THE NAVY COMMANDS.....	18003	18-5
VISITS REQUIRING ACCESS TO SPECIAL COMPARTMENTED INFORMATION (SCI).....	18004	18-5
INVESTIGATIVE AGENCY VISITS.....	18005	18-6
FIGURE		
18-1 SAMPLE VISIT REQUEST.....		18-7

SOP FOR IPSP

CHAPTER 18

VISITOR CONTROL

18000. BASIC POLICY

1. The Commanding General and Commanding Officers are responsible for establishing visitor control procedures within their areas of responsibility to ensure that classified information is adequately safeguarded.

2. The movement of all visitors shall be restricted in such a manner that they cannot either intentionally or accidentally gain access to classified information. Appropriate control measures include the use of assigned escorts, command/section (i.e., after hours, CMCC) visitor logs and providing administrative and physical security measures for areas in which classified information is used or stored. After normal working hours, all personnel assigned to the unit and visitors will log in and out with duty personnel if working in an area where classified material is stored. Visitors will not be allowed access to areas where classified material is stored unless escorted and in the performance of official duties (see paragraph 18005).

3. The control of visitors, to include U.S. Armed Forces personnel, U.S. civilians and foreign national military, civilian and base workers, is the responsibility of all supervisors. All personnel must be indoctrinated by their respective supervisors concerning internal security and the requirement for compliance with the "Need-to-Know" principle. No visitor, U.S. or foreign national, should be allowed free access to office spaces when they are not recognized as being a member of a unit or section.

4. For security purposes, the term visitor applies as follows:

a. A visitor is any person who is not attached to or employed by the command or staff being visited. Examples:

(1) Member of the Division G-3 visiting 9th Marines S-3.

(2) Wife of the Division G-1 visiting husband in office.

(3) A civilian foreign national performing maintenance in a building occupied by a unit/section of the 3d Marine Division.

(4) A military foreign national performing official duties with a unit/section of the 3d Marine Division.

(5) A member of another branch of the U.S. Armed Forces performing official business at 12th Marine Regiment.

18001. GENERAL VISITING. General visiting will be allowed on an unclassified basis only, i.e., no classified areas or information will be shown or divulged to the general public. Should units of the Division hold field meets or open house activities, commanding officers will ensure that sensitive areas such as the unit headquarters, communications facilities, armories, etc. are afforded appropriate increased physical security to limit or deny access to the visiting public.

1. Commanding officers may publish and post orders pertaining to general visiting for areas under their control.
2. General visiting is not authorized in areas where classified material is utilized or stored.
3. General visiting is not authorized in communications facilities or armories.

18002. CONTROL MEASURES. The following control measures apply to all elements of the 3d Marine Division.

1. Local nationals (base workers) whose business is to maintain or repair facilities/equipment will be required to check in with the G-4/designated official or office for subordinate headquarters elements. When G-4/designated personnel or office have ascertained that a base worker is on official business they will be escorted to the appropriate section within the Headquarters building to complete their business. Base workers performing maintenance/repairs inside a military office space will be under constant escort by personnel of that office. When maintenance/repairs are completed, the base worker will be escorted back to the G-4/designated personnel or office, and will be escorted to the nearest exit. After checking in with the G-4/designated personnel or office, base workers may be unescorted when working in passageways, ladderwells, heads, etc. The G-4/designated personnel or office will periodically check on any unescorted base workers.
2. For military office spaces where classified material or information is stored, or in use, the entry of an unknown or uncleared U.S. service member or local national will cause supervisors to secure all classified material (maps, charts, briefing boards, etc.) and terminate discussions of classified information. Moving a discussion or classified material to the next office for convenience is not authorized. Should operational requirements dictate that maintenance/repairs or unofficial visits are untimely, the visitor will be directed to leave and/or maintenance/repairs will be rescheduled.
3. During normal hours of operation, offices with multiple entrances, where classified material is utilized and/or stored, will designate one entrance as the primary means of entering the work spaces. All other entrances will remain locked, but

accessible for use as emergency exits.

18003. CLASSIFIED VISITS TO DEPARTMENT OF THE NAVY COMMANDS

1. Periodically, members of the 3d Marine Division are required to visit other Department of the Navy commands where access to classified information/material is required. When such visits are required, the individual's security manager will ensure that figure 18-1 is completed and forwarded to the commanding officer/security manager of the command to be visited.

2. In keeping with the policy in paragraph 22-10 of reference (c), commanding officers will accept clearances for access to classified information granted to visitors by competent authority. This acceptance extends to the information on the visit request as an authoritative statement of the visitor's status. The information required by paragraphs 18-3.4 (U.S. citizens or immigrant aliens employed by the Executive Branch of the Government) and 18-6 (DOD contractors) of reference (c), provides a sufficient basis for the command being visited to approve or deny a visit. Additional requirements will not be imposed. The commanding officer is not, however, relieved of the responsibility for determining the visitor's "Need-to-Know" or from the duty to withhold classified information when he considers it necessary.

3. Commanding officers may hold the visit request and have the visitor(s) check in with him personally and grant access as required, or attach an access granted endorsement to the visit request and pass it to the cognizant section for identification and appropriate action when the visitor arrives.

4. For the Division Headquarters, formal visit requests involving access to classified material will be validated/endorsed by the Headquarters Battalion Security Manager.

5. Formal visit requests (figure 18-1) are not required for members of the 3d Marine Division when visiting another unit of the Division. An individual's level of security clearance will be certified by his commanding officer per the instructions contained in chapter 24 of this Order.

6. When there is an established working relationship and the clearance level and bounds of "Need-to-Know" of members of the Division are known, a visit request is not necessary. Example: Division G-3 has established working relationship with 4th Marines S-3 over a period of time to include contact via secure STU III.

7. For individuals assigned TAD to a unit of the Division, access to classified material will be granted and recorded per the instructions contained in chapter 24 of this Order.

18004. VISITS REQUIRING ACCESS TO SPECIAL COMPARTMENTED INFORMATION (SCI). The visit request shown in figure 18-1 will

not be used for visits to other commands when access to SCI material is required. All visit requests for members of the 3d Marine Division requiring SCI access, will be prepared and transmitted by the Division Special Security Office (SSO). Visit requests received by any unit of the 3d Marine Division requiring SCI access, will immediately be forwarded to the SSO for appropriate action. SCI material will not be discussed with any visitor without prior approval/validation from the SSO. Security managers can contact the SSO at DSN 622-7336.

18005. INVESTIGATIVE AGENCY VISITS. Certain federal investigative agencies routinely conduct activities within the environs of the 3d Marine Division. Members of these agencies are to be extended cooperation in the conduct of their activities. Members of the agencies listed below are certified to possess a top secret clearance. After presenting the appropriate credentials to unit security managers, they will be granted accompanied access to facilities and classified material that is pertinent to that agencies activities. After presenting their credentials, members of the recognized agencies are exempt from searches of briefcases or other such containers in their possession. The recognized agencies are:

- a. The Naval Criminal Investigative Service.
- b. Marine Corps Counterintelligence.
- c. Criminal Investigative Department.

SOP FOR IPSP

U.S. GOVERNMENT PRINTING OFFICE: 1970-28-207

2

VISIT REQUEST **PRIVACY ACT STATEMENT ON REVERSE** **CHECK ONE**

VISITOR CLEARANCE DATA **REPLY REQUIRED**
 OPNAV MELV/ST (REV. 1-78) BY 8287-LP-021-2222 **REPLY ONLY IF NEGATIVE**

SEE CURRENT EDITION OF OPNAVINST. 2016.1 FOR DETAILED INSTRUCTIONS

FROM: **NAME AND TITLE OF REQUESTING OFFICER**
 Chief of Naval Operations
 Department of the Navy (Op-XXX)
 Washington, DC 20350

NAME OF REQUESTOR
 (Data)
 OFFICER PLANNING BY SECTION
 OF BUREAU TO BE VISITED
 James E. Russell

TO: **NAME AND TITLE OF OFFICER TO BE VISITED**
 Commander
 Naval Systems Command
 Washington, DC 20373

DATE OF VISIT REQUESTED (Data) EXPIRY DATE (Data) GRADE OF OFFICER VISITED
 Secret

REASON FOR VISIT (PLEASE CHECK ONE OR MORE BOXES) (Data)

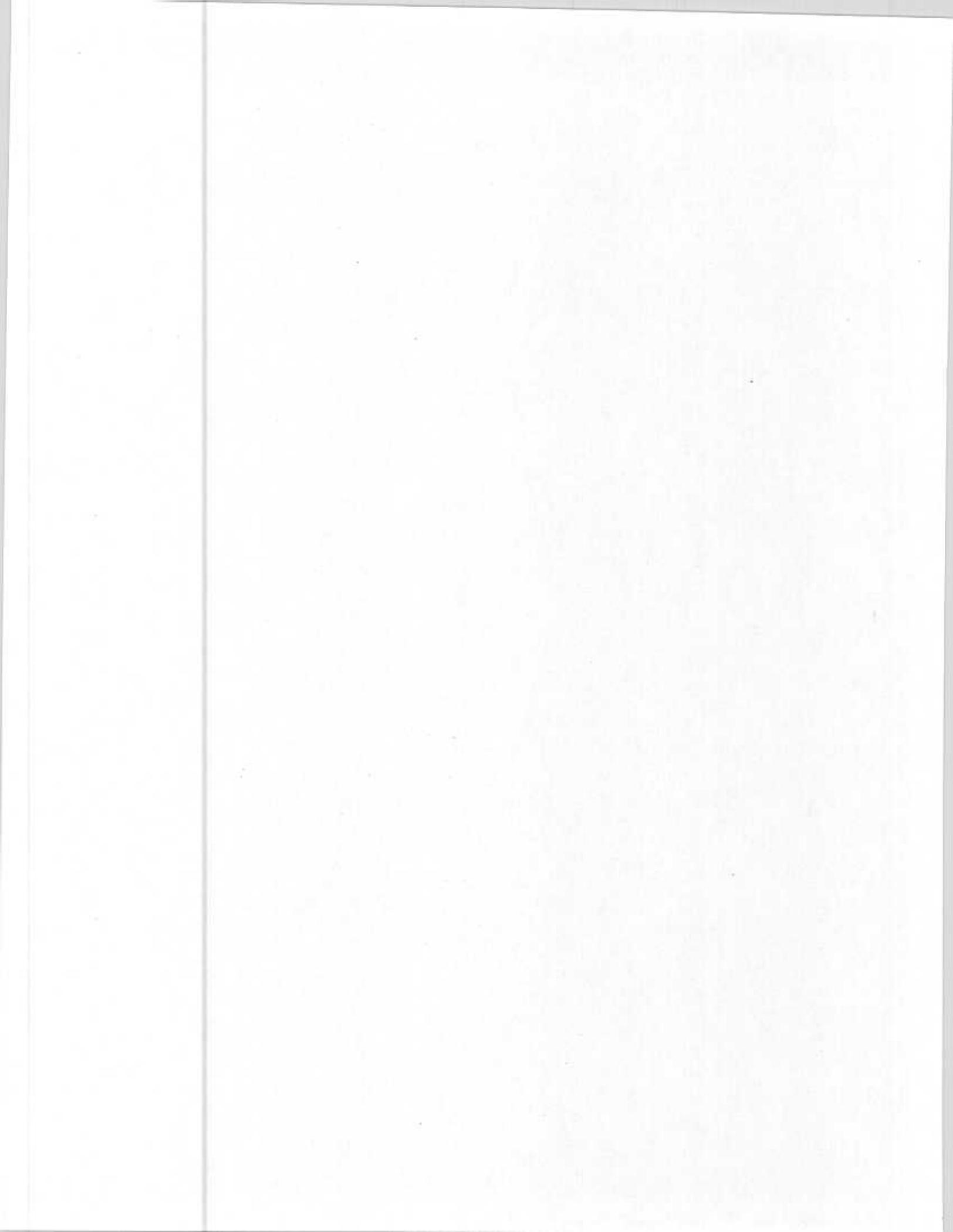
To coordinate classification guidance

NAME, GRADE, TITLE OR POSITION, SOCIAL SECURITY NO.	DATE AND PLACE OF BIRTH	NATIONALITY (CHECK ONE)	LEVEL OF SECURITY CLEARANCE
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	

NAME AND TITLE OF OFFICER AUTHORIZING VISIT AND SIGNATURE
 LCDR Ronald Marshall

SIGNATURE
Ronald Marshall

Figure 18-1. Sample Visit Request

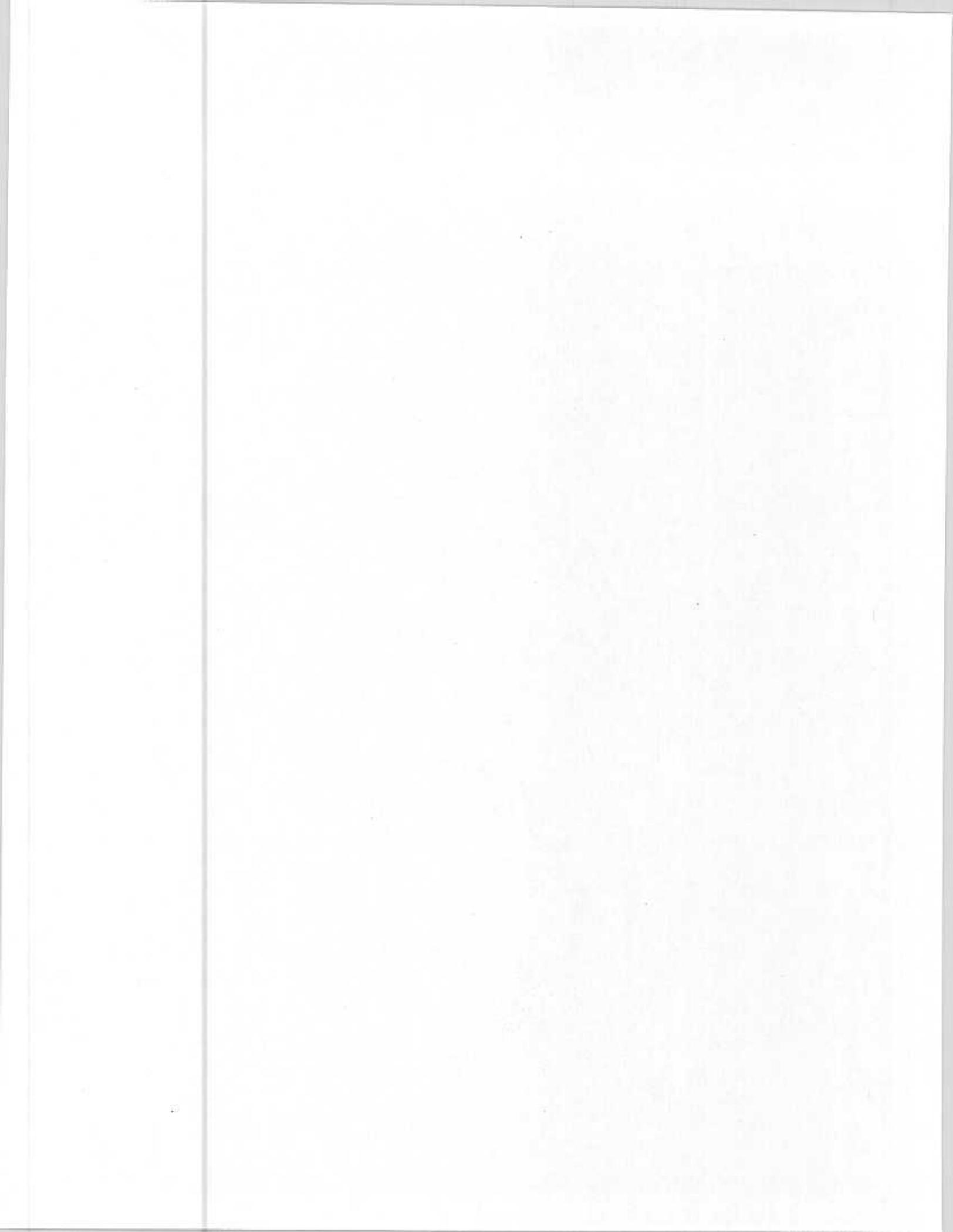


SOP FOR IPSP

CHAPTER 19

MEETINGS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	19000	19-3
RESPONSIBILITY.....	19001	19-3
SECURITY PROCEDURES.....	19002	19-3
SECURITY CLEARANCE CERTIFICATION.....	19003	19-3



SOP FOR IPSP

CHAPTER 19

MEETINGS

19000. BASIC POLICY. Classified information will not be discussed at meetings (conferences, symposia, exhibits, clinics, conventions or gatherings) unless disclosure of the information is clearly consistent with the interests of national security and adequate security measures are taken to control access to the information and prevent its compromise. Detailed guidance for minimum security requirements can be found in chapter 19 of reference (c) and this Order.

19001. RESPONSIBILITY. Heads of General and Special staff sections, and commanding officers are responsible for ensuring that conferences, meetings and working groups they sponsor are not used to discuss classified information unless adequate security measures are taken to control access to the information.

19002. SECURITY PROCEDURES. Security sponsors of meetings where classified information will be discussed are responsible for ensuring the following procedures are followed:

a. Ensure that area(s) in which classified discussions will take place provide adequate security to preclude unauthorized access.

b. Ensure adequate storage facilities and containers are available to safeguard all classified material required at the meeting.

c. Ensure that each attendee has been authorized access to the level of classification involved in the meeting.

d. Ensure that all attendees are on an approved access list and that each individual is admitted only upon proper identification.

e. Ensure that personnel who will disclose classified information are informed of any security limitations to be imposed as result of:

(1) Access level authorized for all attendees.

(2) Need-to-know of all attendees.

(3) Physical security conditions.

f. All sessions must be monitored to ensure discussions remain at the level of classification authorized.

19003. SECURITY CLEARANCE CERTIFICATION. Commanding officers of other organizations will submit security clearance certification

letters or messages to the appropriate security sponsor. The security sponsor will ensure that the unit security manager grants local access to the attendee prior to attending meetings where classified information will be discussed.

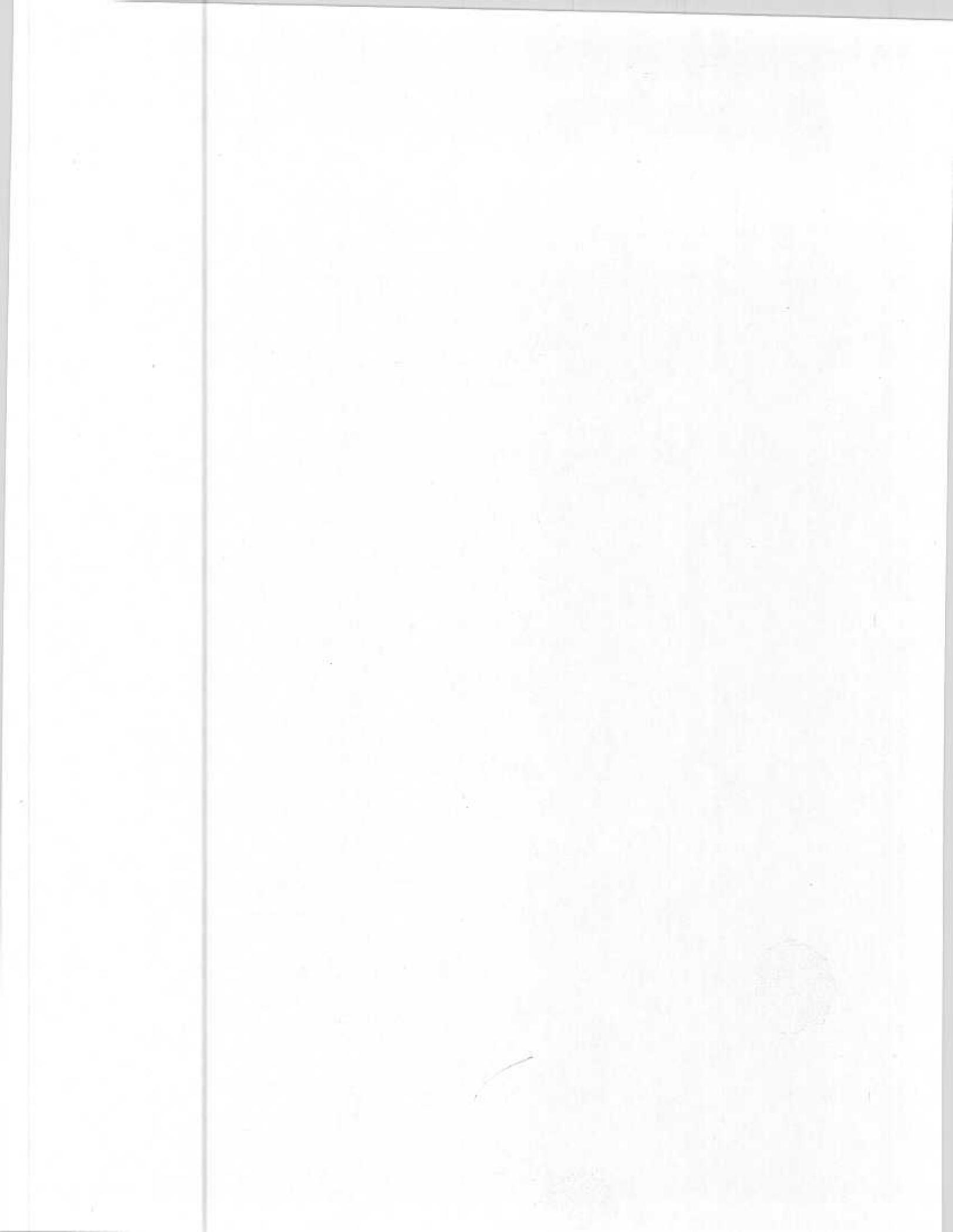
1. Since the security sponsor of a classified meeting is not always the unit security manager, commanding officers will ensure that a copy of all certification messages or letters are provided to the cognizant unit security manager. Local access granted by the cognizant security manager does not need to be recorded.
2. The Headquarters Battalion Security Manager will grant local access for all meetings sponsored by General and Special staff sections of the Division Headquarters.
3. Attendees of meetings where classified information will be discussed are not authorized to hand deliver their own clearance certification.
4. When passing clearance certification to organizations outside the Division, a formal visit request, addressed in chapter 18 of reference (c) and this Order will be prepared by the appropriate commanding officer, unless otherwise directed by the organization to be visited.

SOP FOR IPSP

CHAPTER 20

PERSONNEL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	20000	20-3
CENTRAL ADJUDICATION.....	20001	20-3
CITIZENSHIP.....	20002	20-3



SOP FOR IPSP

CHAPTER 20

PERSONNEL SECURITY POLICY

20000. BASIC POLICY. The security standard applied in determining the eligibility for access to classified information, or assignment to other sensitive duties will be based on all available information. This includes determining if the person's loyalty, reliability and trustworthiness are such that entrusting the individual with classified information or assigning the person to sensitive duties/position is clearly consistent with the interest of national security.

20001. CENTRAL ADJUDICATION. The Department of the Navy Central Adjudication Facility (DON CAF), established at the direction of the Secretary of the Navy, is responsible for making all personnel security determinations, for all military and civilian personnel within the Department of the Navy. DON CAF is the authority for granting, denying, and revoking all security clearances, with the exception that authority is currently delegated to Commander, Naval Intelligence Command (COMNAVINTCOM) and Commander Naval Security Group (COMNAVSECGRU) to grant top secret clearances to those individuals determined eligible for SCI access.

20002. CITIZENSHIP. Only United States citizens are eligible for a security clearance. Only United States citizens are eligible for assignment to sensitive duties or access to classified information. When compelling reasons exist in furtherance of the Department of the Navy mission, including special expertise, a non-U.S. citizen may be assigned to sensitive duties or granted a Limited Access Authorization (LAA) only after the procedures outlined in paragraphs 20-5.6 and 24-7 of reference (c) have been complied with.

SOP FOR IPSP

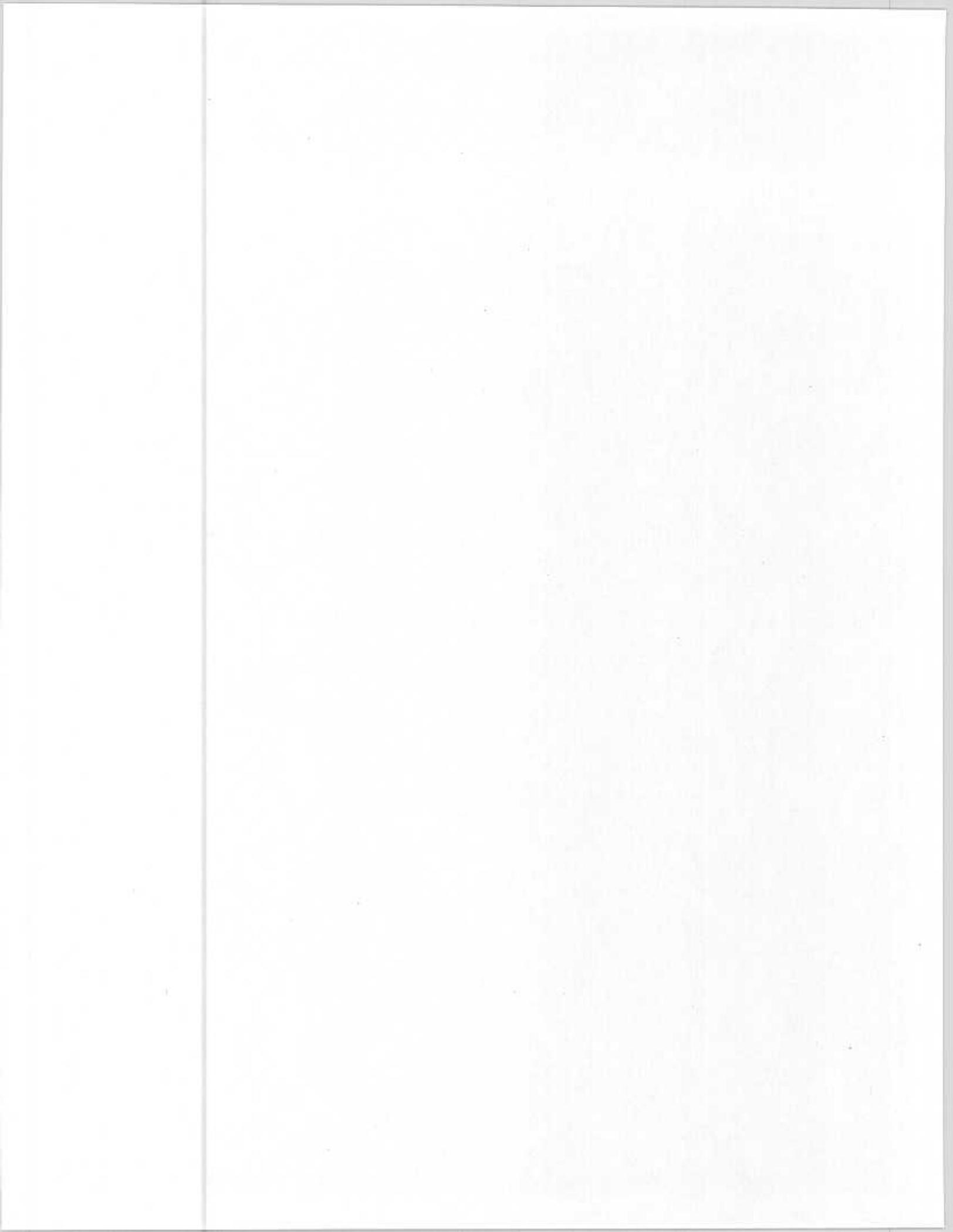
CHAPTER 21

PERSONNEL SECURITY INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	21000	21-3
PREPARATION AND SUBMISSION OF INVESTIGATIONS.....	21001	21-3
RECORDS OF INVESTIGATIONS SUBMITTED.....	21002	21-4
FOLLOW-UP ACTIONS ON INVESTIGATION REQUESTS.....	21003	21-4
REPORTS OF INVESTIGATION.....	21004	21-4
VERIFICATION OF PRIOR INVESTIGATION.....	21005	21-5

FIGURE

21-1	SAMPLE LETTER FOR FORWARDING COPY OF PSI TO NAVY PERSONNEL OFFICE.....	21-7
------	---	------



SOP FOR IPSP

CHAPTER 21

PERSONNEL SECURITY INVESTIGATIONS

21000. BASIC POLICY

1. No member of the Division will be granted access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of their loyalty, reliability and trustworthiness. The initial determination will be based on a personnel security investigation (PSI), appropriate to the access required or to the considerations of the duty or special access program assigned. Detailed guidance pertaining to type investigation requirements are contained in chapter 21 of reference (c).
2. Only the minimum investigation necessary to support a specific level of access or program requirement will be requested.
3. Only commanding officers are authorized to request PSIs on personnel under their jurisdiction.
4. Requests for PSIs must be kept to the absolute minimum. Requests for PSIs will not be submitted on any member of the Division who will be retired, resigned, or separated with less than nine months service remaining.

21001. PREPARATION AND SUBMISSION OF INVESTIGATIONS

1. PSIs will be prepared per the detailed instructions contained in chapter 21 of reference (c).
2. PSIs for access to Special Compartmented Information (SCI) will be prepared in accordance with the detailed instructions contained in reference (c) and supplemented by references (x) and (y).
3. Commanding officers are responsible for preparation, submission and records retention for all PSIs necessary for members of their unit, except for PSIs for SCI access. The Division Special Security Office (SSO) is responsible for preparation, submission and records retention for PSIs related to SCI access.
4. Commanding officers are responsible for preparation, submission, and retention of records of all PSI's necessary for U.S. Navy Personnel attached to their commands. Figure 21-1 will be used to forward a copy of the completed PSI to the Navy Personnel Office (Division Surgeon) for inclusion in the subject's official personnel file. For more details regarding clearance and access for U. S. Navy personnel attached to Marine units, see chapters 23 and 24 of reference (c) and this Order.

21002. RECORDS OF INVESTIGATIONS SUBMITTED

1. Extra copies of PSIs and associated forms/documents will not be reproduced and maintained by units in any fashion other than that directed by paragraph 21-14 of reference (c) and paragraphs 3001 and 4001 of reference (z).
2. The Division SSO will submit to the appropriate commanding officer or Navy Personnel Officer (Division Surgeon), a copy of the submitted PSI and DD Form 1879 (for SCI access) for inclusion in official personnel files.
3. Roughs, work sheets or other forms used to prepare a PSI will be returned to the subject of the investigation for final disposition. When a PSI is completed, one copy may be provided to the individual for his or her personal records.

21003. FOLLOW-UP ACTIONS ON INVESTIGATION REQUESTS

1. All follow-up actions pertaining to PSI requests will be performed per the instructions contained in paragraph 21-15 of chapter 21 of reference (c). Follow-up actions include:
 - a. Rejection of investigation request.
 - b. ENTNAC follow-up.
 - c. Cancellation of investigation request.
 - d. Transfer of the subject of investigation.
 - e. Tracer action.
2. Unit security managers will ensure that tracer action is not initiated for a PSI until sufficient time has elapsed for completion of the PSI. Paragraph 21-15.5.c of reference (c), identifies minimum times required to complete different types of investigations. Tracer action for Marines will be initiated via the MMS per references (c), (aa) and (bb).
3. Tracer action for investigations pertaining to U.S. Navy personnel attached to Marine units will be initiated by the Navy Personnel Office (Division Surgeon) after receipt of a written request from the appropriate unit security manager.
4. Tracer action for investigations related to SCI access will be initiated only by the Division SSO.

21004. REPORTS OF INVESTIGATION

1. The Defense Investigative Service (DIS) reports the results of PSIs and Periodic Reviews (PR) for assignments other than those

involving SCI access, to DON CAF for security clearance adjudication. If a Report of Investigation (ROI) is inadvertently returned to the requester by DIS, the requester will immediately forward it to DON CAF.

2. DIS reports PSIs and PRs for access to SCI to COMNAVINTCOM or COMNAVSECGRU for adjudication. If an ROI is inadvertently returned to the requester by DIS, the requester will immediately forward it to COMNAVINTCOM or COMNAVSECGRU.

21005. VERIFICATION OF PRIOR INVESTIGATION

1. In the absence of a valid certification of documentation of completed investigation in a person's record, and when clear indications exist that a prior investigation has been conducted which would still be valid for current needs, the following procedures should be followed to verify the existence of the prior investigation:

a. For U.S. Navy personnel:

(1) The unit security manager will request the Navy Personnel Office (Division Surgeon) to check the subject's OPNAV 5520/20, ODCR, EDVR or SDS. If evidence of valid security clearance eligibility is found, the command may grant interim clearance and submit a request for security clearance to DON CAF via the Navy Personnel Office.

(2) If no clearance eligibility data is found in ODCR, EDVR or SDS, but there is an indication that an investigation has been completed; the unit security manager can request that the Navy Personnel Office submit a clearance determination to DON CAF. While awaiting DON CAF's response to the clearance determination, an interim clearance cannot be granted. In the absence of evidence of a completed investigation, submit the appropriate PSI request per paragraph 21-14 of reference (c). After the PSI has been submitted to DIS, an interim clearance may be granted per paragraph 23-3 of reference (c).

(3) If clearance eligibility data in ODCR/EDVR/SDS indicates the individual's clearance has been denied or revoked, the command must either cease considering that individual for clearance, or if reason exists to believe that the individual is no longer subject to the factors which resulted in denial or revocation, follow the procedures in paragraph 23-10 of reference (c) for reestablishing clearance eligibility.

b. For U.S. Marine Corps personnel:

(1) Verification of prior investigation will be made utilizing MMS.

(2) If a record of investigation is found utilizing MMS, but no clearance "eligibility" is available, request Clearance Status/Record Update per the instructions contained in paragraph 1118.1 of reference (cc). While awaiting DON CAF's response, an interim clearance cannot be issued.

(3) Based on the response from DON CAF, see paragraph 9106.24 of reference (aa) for examples of MMS Diary Feedback Reports (DFR), take action as directed or authorized by DON CAF.

SOP FOR IPSP

HEADING

5520
ID SYMBOL
(DATE)

From: Commanding Officer, (Unit)
To: Navy Personnel Officer, 3d Marine Division (Div Surg)
Subj: REQUEST FOR SECRET SECURITY CLEARANCE CASE OF HM2 SMITH,
J. D. 123 45 6789/USN

Ref: (a) OPNAVINST 5510.1
(b) DivO P5510.9

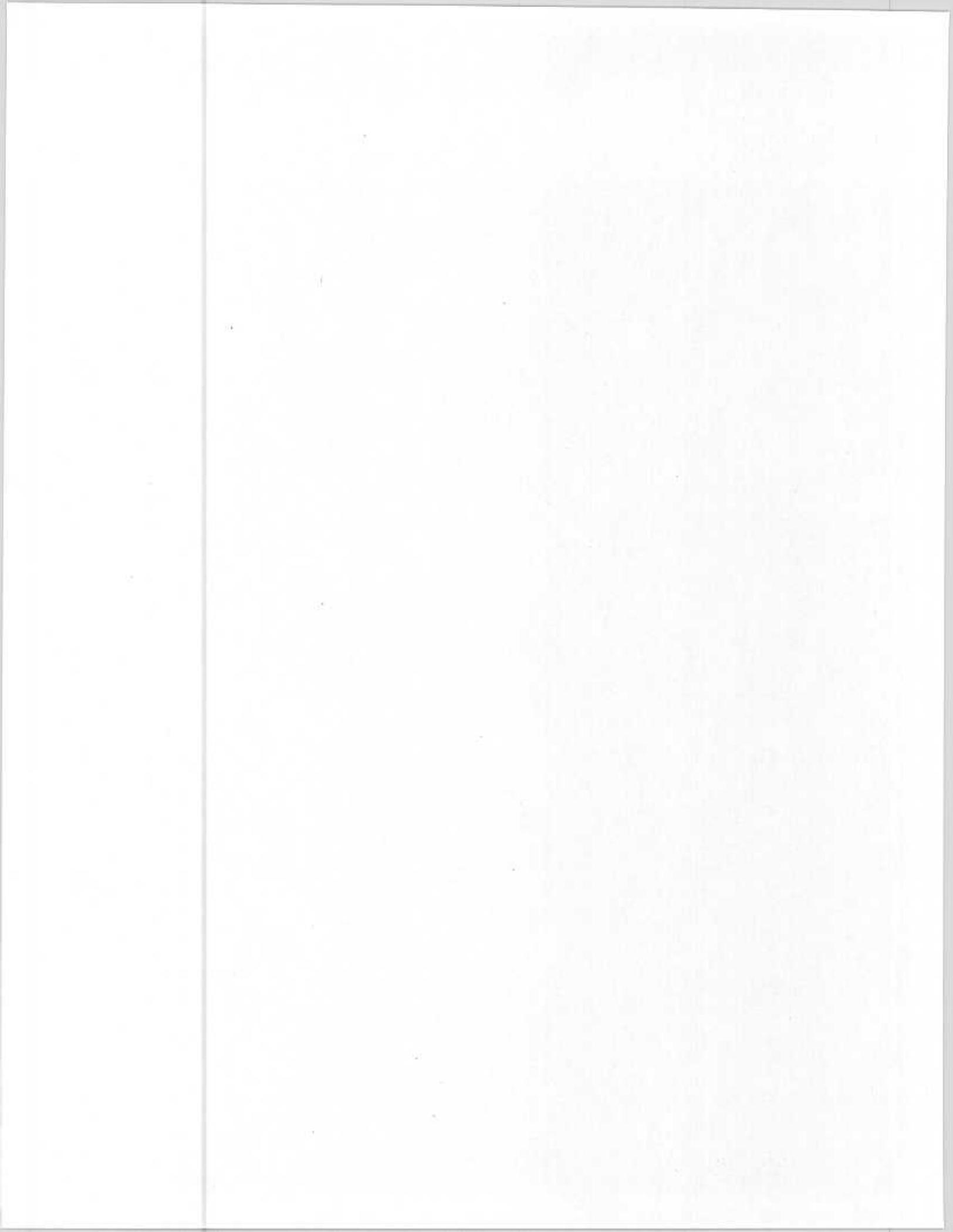
Encl: (1) DD Form 398-2

1. Per the references, a secret security clearance is requested for SNM. The enclosure is forwarded for inclusion in SNM's personnel file.

2. SNM granted interim secret security clearance on 920818.

SIGNATURE

Figure 21-1. Sample Letter For Forwarding Copy Of PSI
To Navy Personnel Office.



SOP FOR IPSP

CHAPTER 22

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	22000	22-3
PERSONNEL SECURITY DETERMINATION AUTHORITIES.....	22001	22-3
UNFAVORABLE PERSONNEL SECURITY ACTIONS.....	22002	22-3
UNFAVORABLE DETERMINATION NOTIFICATION AND APPEAL PROCESS.....	22003	22-3
CONTINUOUS EVALUATION OF ELIGIBILITY.....	22004	22-3
CERTIFICATION OF SECURITY CLEARANCE AND ACCESS.....	22005	22-4

FIGURE

22-1	SAMPLE LETTER CONTINUOUS EVALUATION OF ELIGIBILITY.....	22-5
------	--	------

SOP FOR IPSP

CHAPTER 22

PERSONNEL SECURITY DETERMINATIONS

22000. BASIC POLICY. The principle objective of the personnel security determination is to assure selection of persons who meet the standards addressed in the current edition of OPNAVINST 5510.1. In making this determination, all information favorable and unfavorable is to be considered and assessed. In all determinations, the protection of national security will be the paramount determinant. Commanding officers and unit security managers should be thoroughly familiar with the contents of paragraph 22-2 and Exhibit 22A of reference (c) when making security determinations.

22001. PERSONNEL SECURITY DETERMINATION AUTHORITIES. Authority to make personnel security determinations has been delegated by the Chief of Naval Operations (OP-09N) to commanding officers. Responsibilities associated with this delegation of authority are contained in paragraph 22-3.1.h of reference (c). Commanding officers and security managers should be thoroughly familiar with these responsibilities. With the exception of special access programs addressed in paragraph 23-4 of reference (c), only DON CAF has the authority to grant a final security clearance.

22002. UNFAVORABLE PERSONNEL SECURITY ACTIONS. Paragraph 22-6 of reference (c) addresses unfavorable personnel security actions. Commanding officers and security managers should be thoroughly familiar with the provisions of this paragraph and associated action required.

22003. UNFAVORABLE DETERMINATION NOTIFICATION AND APPEAL PROCESS. Paragraph 22-7 of reference (c) addresses unfavorable determination notification by adjudication authorities and the appeal process. Commanding officers and security managers should be thoroughly familiar with the provisions of this paragraph and associated action required.

22004. CONTINUOUS EVALUATION OF ELIGIBILITY

1. Commanding officers are responsible for continuously evaluating access eligibility for each member of their command. Commanding officers are required to establish and administer a program for continuous evaluation. Any potentially significant information which could place in question an individual's loyalty, reliability, or trustworthiness, and any significant personnel security factors found in Exhibits 21K and 22A of reference (c) will be reported to either DON CAF or, if the individual has access to SCI, to CONNAVINTCOM or COMNAVSECGRU.

a. Reports intended for DON CAF will be prepared per the detailed instructions contained in references (c) and (bb).

b. Reports intended for COMNAVINTCOM or COMNAVSECGRU will be prepared and submitted per applicable directives by the Division Special Security Office.

2. Heads of General and Special staff sections, company commanders, officers-in-charge, legal officers, medical officers and work section supervisors must ensure that questionable or derogatory information reflecting on an individual's eligibility is brought to the attention of the appropriate unit security manager immediately. Each individual identified above will coordinate with the others as appropriate, to ensure complete understanding of all issues involved concerning questionable or derogatory information. The unit security manager is the primary coordinating authority and will be made aware of all matters which might affect an individual's eligibility to maintain a security clearance.

3. Unit security managers will manage their unit's continuous evaluation of eligibility program. Unit security managers will ensure that personnel identified in paragraph 22004.2, are provided with a copy of Exhibits 21K, 22A and paragraph 22-2.2 of reference (c), and are thoroughly briefed on their responsibilities to report questionable or derogatory information pertaining to personnel in their section or unit.

4. On at least a quarterly basis, unit security managers will prepare and distribute figure 22-1 to all work sections that routinely process or maintain classified material. Responses from individual work sections will be maintained by the unit security manager for no less than one year. Questionable or derogatory information need not be included in the sections response. Security managers will be informed verbally of questionable or derogatory information. Security managers will make a determination concerning the information brought to their attention, and may direct a written report with supporting documentation be provided if necessary.

22005. VALIDITY AND RECIPROCAL ACCEPTANCE OF PERSONNEL SECURITY DETERMINATION. A personnel security clearance, granted by an authority of the Department of Defense, remains valid and will be mutually and reciprocally accepted within the Department of Defense. Occasions that require certification of clearance include classified visits, meetings or infrequent visits to conduct business. Within the environs of the 3d Marine Division, formal visit requests addressed in chapter 18 of this Order, will not be utilized to conduct normal business. Within the Division, certification letters or messages will be utilized. For further details regarding this subject, see Chapters 23 and 24 of this Order.

SOP FOR IPSP

HEADING

5520
SecMgr
Date

From: Security Manager
To: Section Head

Subj: CONTINUOUS EVALUATION OF ELIGIBILITY

Ref: (a) OPNAVINST 5510.1H
(b) DivO P5510.9

Encl: (1) Section personnel granted access to classified information

1. Per the references, personnel listed in the enclosure must be continuously evaluated for eligibility to hold a security clearance. Your evaluation should include all available information known that could adversely affect each individual's eligibility to hold a security clearance. Exhibits 21K, 22A and paragraph 22-2.2 of reference (a) should be reviewed before responding to this letter.
2. After reviewing the material listed in the paragraph above, you will take the following actions:
 - a. Identify personnel listed in the enclosure whose duties still require clearance and access at the level indicated.
 - b. Identify personnel reassigned to new duties within the section who require a change in their level of clearance and access.
 - c. Identify personnel in your section whose duties require access to classified information, but are not included in the enclosure. Submit the appropriate request for clearance and access.
 - d. Identify personnel listed in the enclosure who are no longer assigned to your section.
3. Annotate the enclosure as necessary and return it to the Security Manager by (Date) for appropriate action.

SOP FOR IPSP

Subj: CONTINUOUS EVALUATION OF ELIGIBILITY

4. Questionable or derogatory information concerning any member of your section, should be brought to the attention of the Security Manager immediately.

SIGNATURE

Figure 22-1. Sample Letter Continuous Evaluation Of Eligibility
--Continued

SOP FOR IPSP

CHAPTER 23

CLEARANCE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	23000	23-3
CLEARANCE ELIGIBILITY.....	23001	23-3
REQUEST FOR CLEARANCE AND ACCESS.....	23002	23-4
INTERIM SECURITY CLEARANCE.....	23003	23-4
FINAL CLEARANCE.....	23004	23-7
SPECIAL ACCESS PROGRAMS.....	23005	23-7
SCI ACCESS ELIGIBILITY.....	23006	23-8
COMMANDING OFFICER CLEARANCE.....	23007	23-8
ADMINISTRATIVE WITHDRAWAL OR ADJUSTMENT OF CLEARANCE.....	23008	23-8
DENIAL OR REVOCATION OF SECURITY CLEARANCE FOR CAUSE.....	23009	23-9
RECORDS.....	23010	23-10
SECURITY CLEARANCE ROSTER.....	23011	23-10

FIGURE

23-1	SAMPLE LETTER FOR INTERIM CLEARANCE AND ACCESS.....	23-12
23-2	SAMPLE LOCAL RECORDS CHECK FOR MARINES.....	23-13
23-3	SAMPLE LOCAL RECORDS CHECK FOR SAILORS.....	23-14
23-4	SAMPLE LETTER TO NAVY PERSONNEL OFFICE REQUESTING SECURITY CLEARANCE.....	23-15
23-5	SAMPLE LETTER FOR EXTENDED INTERIM CLEARANCE AND ACCESS.....	23-16

SOP FOR IPSP

	<u>PAGE</u>
23-6 SAMPLE LETTER FOR ADMINISTRATIVE REDUCTION OF INTERIM TOP SECRET CLEARANCE TO SECRET.....	23-17
23-7 SAMPLE LETTER FOR FINAL CLEARANCE AND ACCESS.....	23-18
23-8 SAMPLE LETTER FOR FINAL CLEARANCE AND ACCESS FOR SPECIAL ACCESS PROGRAM.....	23-19
23-9 SAMPLE LETTER FAVORABLE ELIGIBILITY DETERMINATION FOR SCI ACCESS.....	23-20

SOP FOR IPSP

CHAPTER 23

CLEARANCE

23000. BASIC POLICY

1. A personnel security clearance will be issued to individuals by DON CAF, or other designated clearance authority as authorized in reference (c), only at the request of his/her command and upon affirmation that granting such clearance is clearly consistent with the interests of national security. For the 3d Marine Division, officials authorized to issue a security clearance are the Commanding Officers of regiments, groups (i.e. CSG) and battalions. These Commanding Officers may delegate this authority to unit security managers and assistant security managers (if assigned), as long as the security manager and assistant meet the criteria established in Chapter 2 of reference (c). See paragraph 2-11.4 of reference (c) for restrictions on issuing security clearances by enlisted assistant security managers. Security clearances will not be issued to those personnel identified in paragraph 23-2 of reference (c).

2. A personnel security clearance is an administrative determination that an individual is eligible for access to classified information at a specified level of classification. A security clearance is not de facto authorization for an individual to access classified information. Authorization to access classified information is a separate determination as to whether an individual who has the requisite security clearance also has a need to access the information in the performance of official duties.

3. A Classified Information Nondisclosure Agreement (Standard Form 312) shown in Exhibit 24B of reference (c), must be executed by all Division personnel as a condition of access to classified information. Execution of an SF 312 will be accomplished prior to clearance and access being granted to any member of the Division. For Marines, execution of SF 312 will be recorded on page 11 of the Officer Qualification Record (OQR) and Service Record Book (SRB) per the instructions contained in references (c) and (z). For U.S. Navy personnel attached to Marine units, execution of SF 312 will be accomplished by the unit to which attached. The completed SF 312 will be forwarded to the Navy Personnel Office (Division Surgeon), for recording per reference (c) and other applicable directives. For personnel who have previously executed an SF 189, SF 189-A or other nondisclosure agreements (Nda) allowed by the National Security Council (NSC), execution of SF 312 is not necessary.

23001. CLEARANCE ELIGIBILITY. Only U.S. citizens are eligible for a security clearance. Although non-U.S. citizens are not eligible for security clearance, access to classified information may be justified for compelling reasons in furtherance of the unit

mission, including special expertise when justified. Non-U.S. citizens may be considered for limited access authorization (LAA) in accordance with the conditions outlined in paragraph 24-7 of reference (c). Requests for LAA will be submitted in writing per the instructions contained in paragraph 24-7.2 of reference (c) via the Commanding General, 3d Marine Division (Security Manager).

23002. REQUEST FOR CLEARANCE AND ACCESS

1. Section heads will submit in writing requests for clearance and access to the unit commanding officer/security manager. Requests for clearance and access will include the following information:

- a. Last name and initials.
- b. Rank.
- c. Social security number.
- d. Level of clearance and access required.

2. Units may identify clearance and access requirements based on the billet to which an individual is assigned. If this method of identifying clearance and access requirements is utilized, security managers will ensure that administrative procedures are developed and included in appropriate turnover folder/desktop procedures maintained by the units personnel section.

3. Requests for clearance and access for individuals assigned to General and Special staff sections of the Division Headquarters will be submitted to the Commanding Officer, Headquarters Battalion (Security Manager).

23003. INTERIM SECURITY CLEARANCE. An interim security clearance is granted temporarily, pending completion of full investigative requirements for different levels of clearance or special access requirements outlined in chapter 21 of reference (c), or revalidation of security clearance upon transfer.

1. Interim clearances are granted by commanding officers and recorded for Marines and Sailors, by using figure 23-1. Per the instructions contained in references (c) and (bb), prior to granting an interim clearance for 180 days, the following actions will be completed.

- a. For Marines:
 - (1) Determine level of access required.
 - (2) Confirm clearance eligibility by viewing the MMS

Visual Inquiry System (VIS) VFO3 screen, (see subparagraph 23003.(c)).

- (3) Confirm U.S. citizenship.
 - (4) Review OQR/SRB as appropriate.
 - (5) Submit figure 23-2 , Local Records Checks (LRC) NAVMC 10482, for review of medical records.
 - (6) Submit figure 23-2 LRC, to Provost Marshals Office (PMO) Attn: MILPENS for review of records.
 - (7) Submit appropriate security clearance unit diary entry to DON CAF, see paragraph 1118.1 of reference (cc).
 - (8) Brief individual per chapter 3 of reference (c).
- b. For U.S. Navy personnel attached to Marine units:
- (1) Determine level of access required.
 - (2) Confirm clearance eligibility and U.S. citizenship with Navy Personnel Office (DSN 622-9264). Navy Personnel Office will view EDVR or ODCR and official personnel file. Confirmation of clearance eligibility and U.S. citizenship will be returned within 48 hours, (see subparagraph 23002.c).
 - (3) Submit LRC figure 23-3, for review of medical/dental records.
 - (4) Submit LRC figure 23-3, for review of PMO records.
 - (5) Unit prepares figure 23-4, letter requesting Navy Personnel Office request clearance for SNM from DON CAF.
 - (6) Navy Personnel Office reviews LRC results and screens official personnel file.
 - (7) Navy Personnel Office prepares security clearance request (OPNAV 5510/413) Exhibit 21M of reference (c), and submits to DON CAF with Marine unit as "INFO ADDEE". Date interim clearance is issued is included on line 14 of the message. OPNAV 5510/413 will not be used to request a security clearance from DON CAF for Marines.
 - (8) Navy Personnel Office endorses unit's clearance request letter (figure 23-4) and forwards LRCs to the unit.
 - (9) Unit receives information copy of OPNAV 5510/413. Unit prepares figure 23-1 to coincide with interim clearance date on line 14 of message.

(10) Brief individual per chapter 3 of reference (c).

c. When a PSI contains certain data requiring further investigation or other action, adjudication of the PSI and clearance eligibility determination will be held in abeyance pending completion of such investigation or action. DON CAF will code the access/clearance as "J" (no clearance required - file created requiring review for clearance eligibility determination). When code "J" or no clearance eligibility is reflected on PCS orders, ODCR, EDVR, SDS, MMS or Navy Civilian Personnel Data System (NCPDS), commanding officers must submit a request for a final clearance to DON CAF via MMS for Marines, via OPNAV 5510/413 for Sailors, for a security clearance determination. Commanding officers may not, in this case, grant an interim clearance and access until authorized by DON CAF.

2. Commanding officers may extend an interim security clearance for an additional 180 days per paragraph 23-3 of reference (c).

a. For Marines:

(1) If DON CAF has not issued a final clearance after 150 days from date initial interim clearance was issued, make unit diary entry per paragraph 1118.1 of reference (cc), Code "J".

(2) Grant extended interim clearance using figure 23-5.

b. For U.S. Navy personnel attached to Marine units:

(1) If DON CAF has not issued a final clearance after 150 days from date initial interim clearance was issued, unit prepares letter requesting Navy Personnel Office initiate tracer action and notify DON CAF of extended interim clearance.

(2) Navy Personnel Office prepares OPNAV 5510/413 requesting tracer action. On line 16 of OPNAV 5510/413 the following statement is entered, "Interim Clearance has been extended 180 days". Requesting unit is included as "INFO ADDEE" on message.

(3) Grant extended interim clearance using figure 23-5.

3. Commanding officers may grant an interim top secret clearance for 180 days on the basis of a favorable ENTNAC, NAC, provided an SSBI is requested and all actions addressed in paragraph 23003.1 have been completed.

4. When an interim top secret clearance is based on a BI, SBI or the new SSBI that is older than five years, the commanding officer will ensure that the required PR is submitted by the individual within 30 days of issuing the interim clearance. If a PR is not submitted within 30 days, the interim top secret clearance is no longer valid and will be administratively lowered to secret by the

commanding officer using figure 23-6. An appropriate unit diary entry (Code "B") will be made per reference (cc).

5. When an individual is transferred from a command, the individual's requirement for clearance and access at that command no longer exists. The individual's clearance eligibility, however, remains unchanged. When the individual requires a clearance at his/her next command, the gaining command, after completing the actions directed in paragraph 23003.1, will submit a request to DON CAF to have the individual's security clearance revalidated. Revalidation requires no additional action other than that shown in paragraph 23003.1. DON CAF will peruse the individual's file and confirm if security clearance eligibility remains valid. If eligibility has changed or a new investigation or PR is required, DON CAF will notify Marine units via the MMS with a Diary Feed Back Report (DFR). Paragraph 9106.24 of reference (aa) identifies different DFR messages sent via MMS from DON CAF.

6. Unit security managers will ensure that unit diary personnel are made aware of the significance of DON CAF generated DFRs and that they are delivered as soon as possible to the security manager for action.

23004. FINAL CLEARANCE. When a final security clearance has been granted by DON CAF, COMNAVINTCOM or COMNAVSECGRU, commanding officers will utilize figure 23-7 to record the final clearance for Marines. For U.S. Navy personnel, commanding officers may prepare figure 23-7, or utilize the message received from the adjudication authority for inclusion in unit security files.

23005. SPECIAL ACCESS PROGRAMS. When an individual is transferred to a position requiring access to classified information in a special access program (i.e., NATO, SIOP-ESI, PRP, NNPI, CNWDI, CRYPTO), after completing the action directed in paragraph 23003.1, the gaining commander has been delegated the authority to grant the appropriate final clearance, not to exceed the level of eligibility authorized, when submitting to DON CAF a request for clearance revalidation (see paragraph 1118.1 of reference (cc) concerning unit diary request Codes "D" and "E").

1. Under no circumstances will an individual be granted a final clearance or afforded access to special access program material, until a request for final clearance has been forwarded to DON CAF.

2. Unit security managers will ensure special access program indoctrination/briefing requirements are complied with, and appropriate records are on file prior to granting access.

3. The final security clearance issued by the commanding officer will be recorded using figure 23-8.

23006. SCI ACCESS ELIGIBILITY. The SSO will inform the appropriate unit security manager when a favorable determination of eligibility for access to SCI has been made, and a final top secret clearance granted/established by COMNAVINTCOM or COMNAVSECGRU (including transfer in status) using figure 23-9.

1. When a favorable determination of eligibility is made, COMNAVINTCOM or COMNAVSECGRU will notify DON CAF of the fact, and automatically enter a top secret clearance in the Automated Security Clearance System. This top secret clearance will normally post on the individual's VFO3 screen with a "T" code on the clearance held line. Unit security managers will not have to request a top secret security clearance from DON CAF via the MMS for the individual as shown in paragraph 23003.1.(7). However, all other action required in paragraph 23003 will be completed, prior to granting access using figure 23-7.

2. Briefing and indoctrination requirements for SCI access will be performed and appropriate records maintained by the SSO.

3. SCI access eligibility, and being granted access to SCI material does not constitute authorization for access to other classified information maintained by the command. Unit security managers will ensure that top secret genser access is granted by the commanding officer before individuals are allowed access to genser classified material.

4. To allow access to genser classified material without the appropriate level of access granted by the commanding officer, constitutes a violation of the regulations contained in reference (c) and this Order. Such violations will be investigated and reported per the instructions contained in chapter 4 of reference (c) and this Order.

23007. COMMANDING OFFICER'S CLEARANCE. Procedures for a commanding officer's clearance are addressed in chapter 23, paragraph 23-4.8 of reference (c). There is no requirement to locally record a commanding officer's clearance. However, the appropriate level of clearance will be requested via the MMS from DON CAF per the instructions contained in paragraph 1118.1 of reference (cc), unless the commanding officer has already been granted a final top secret clearance due to SCI access eligibility addressed in paragraph 23006. For the 3d Marine Division, the instructions in this paragraph also apply to the individual filling the billets of Assistant Division Commander and Chief of Staff.

23008. ADMINISTRATIVE WITHDRAWAL OR ADJUSTMENT OF CLEARANCE

1. Commanding officers are required to administratively withdraw an individual's security clearance when it is no longer required for performance of official duties at that command. The command will debrief the individual in accordance with paragraph 3-12 of

reference (c) and execute a Security Termination Statement (OPNAV Form 5511/14), shown in Exhibit 3D of reference (c). The completed Security Termination Statement will be filed in the individual's OQR/SRB per the instructions contained in references (c) and (z). For Marines of the Division, administrative withdrawal of a security clearance will be reported via a unit diary entry (code "F"), per reference (cc).

2. The administrative withdrawal or lowering of a security clearance is not appropriate or authorized when prompted by developed derogatory information on an individual (i.e., for cause). In these cases, the derogatory information will be reported immediately to DON CAF via OPNAV 5510/413 for U.S. Navy personnel, and for Marines, per the instructions contained in reference (bb).

3. Commanding officers will not usually administratively withdraw a security clearance for U.S. Navy personnel attached to their command. Should such action be contemplated, the unit security manager will contact the Navy Personnel Office (Division Surgeon) for guidance and coordination.

23009. DENIAL OR REVOCATION OF SECURITY CLEARANCE FOR CAUSE

1. In the event DON CAF determines that an individual either fails or ceases to meet the criteria for a security clearance as set forth in paragraph 22-2 of reference (c), DON CAF will deny or revoke the individual's security clearance eligibility for cause. Should this occur, unit security managers will usually receive notification via the MMS in the form of a Diary Feed Back Report (DFR). Unit security managers will take the appropriate action directed by DON CAF in all such instances.

2. Commanding officers may deny or revoke an individual's security clearance for cause, should it be determined that an individual no longer meets security clearance eligibility criteria in paragraph 22-2 of reference (c). The revocation will be reported to DON CAF using the report format contained in enclosure (3) of reference (bb). Per the instructions contained in reference (bb), a unit diary entry (Code "G"), see reference (cc) is also required.

3. Per references (c) and (bb), commanding officers will revoke an individual's security clearance when a military member is adjudged a punitive discharge, incarcerated as the result of a conviction for a criminal offense, or declared a deserter. The commanding officer will revoke their security clearance eligibility immediately and without regard to administrative due process. The report of revocation will be forwarded to DON CAF and CMC (MMRB). In situations where an individual has held SCI access, an information copy will be forwarded to COMNAVINTCOM or COMNAVSECGRU, after coordination with the SSO. A unit diary entry (Code "H") to DON CAF is also required.

4. Revocation of a security clearance for U. S. Navy personnel attached to Marine units, will be accomplished in accordance with the directions contained in reference (c). Unit security managers will coordinate such action with the Navy Personnel Office (Division Surgeon).

23010. RECORDS. The following records will be maintained on each individual granted clearance and access to classified material.

a. For SCI clearance and access, the Division SSO will maintain individual files which will include all pertinent records required by references (c), (x) and (y).

b. For genser clearance and access, unit security managers will maintain individual files which will include at a minimum, the information listed below. This file will be maintained for a period of two years after the individual has been transferred, than destroyed.

- (1) Work section request for security clearance.
- (2) Copy of VFO3 screen showing clearance eligibility.
- (3) LRC with results of review of medical/dental records.
- (4) LRC with results of review of records by PMO.
- (5) Interim clearance granted by the command and extension if applicable.
- (6) Notification of final clearance issued by DON CAF.
- (7) Any DFRs related to the individual received via the MMS from DON CAF.
- (8) Record of all briefings received by the individual related to his or her clearance and access.

Unit security managers are reminded that some information made available by medical and PMO local records checks, which is reviewed prior to granting clearance, may need to be omitted from security files under provisions of the Privacy Act.

23011. SECURITY CLEARANCE ROSTER

1. Unit security manager will ensure that their unit receives, on at least a monthly basis, a security clearance roster generated by the Manpower Management Information System Support Office (MISSO). The security clearance roster will be utilized as a management tool and as a means of recording all clearance action taken for members of the command.

2. The roster will be annotated (in pencil) with the following information.

- a. Interim clearances issued (i.e., "ITS", "IS").
- b. Administrative reduction, termination or revocation of clearance (i.e., "F", "G", "H").
- c. Requests for security clearances submitted to DON CAF via unit diary entry or OPNAV 5510/413 for U.S. Navy personnel (i.e. "B", "C").
- d. New joins not listed as of last printing (include last name, initials and social security number).
- e. Personnel transferred will be neatly lined out.

3. When a new roster is received, it will be reconciled against the old roster. Pencil entries on the old roster that have not posted on the new roster will be transcribed to the new roster. When the new roster has been completely updated, the old roster will be destroyed.

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: INTERIM CLEARANCE AND ACCESS CASE OF SSGT JONES, J. J.
123 45 6789/0311 USMC

Ref: (a) OPNAVINST 5510.1_
(b) Divo P5510.9_

1. Per the references, an interim (level) security clearance and access is granted for a period of 180 days.
2. SNM has received a security orientation briefing in accordance with the references. Work section supervisors are reminded that SNM must receive a briefing on security procedures applicable to the work section in accordance with the references.
3. This interim (level) security clearance expires on (date).

(Include the following as paragraph 4 if applicable)
4. This interim top secret security clearance is based on a BI/SBI/SSBI that is older than five (5) years. You are directed to submit the appropriate PSI/PR per the instructions contained in the references within thirty (30) days.

SIGNATURE

Copy to:
SNM
CMCC
Security Files

Figure 23-1. Sample Letter For Interim Clearance And Access

SOP FOR IPSP



UNITED STATES MARINE CORPS
 HEADQUARTERS BATTALION
 1ST MARINE DIVISION (1ST MARDIV), FLEET MARINE FORCE
 FMF 20000
 070 AF 20000-20000

LOCAL RECORDS CHECK (1800)
 MAYMC 1044C (Rev. 3-78) (Previous edition will be void)
 BY 000-00-000-000 USE 01

DATE: _____

NAME (Last, First, Middle) JONES, John J.		SSN 123 45 6789	GRADE SSgt	MOB
ORGANIZATION HQ Co, 4th Marine Regt.				
DATE OF BIRTH 651010	PLACE OF BIRTH San Diego, California		CITIZENSHIP U. S.	
NAME OF SPOUSE (Last, First, Middle)		DATE OF BIRTH	PLACE OF BIRTH	CITIZENSHIP
CLEARANCE STATUS (Dispers)	BASIS	COMPLETED BY (Agency)		DATE COMPLETED

PURPOSE FOR REQUESTING LOCAL RECORDS CHECK

RESULTS OF COMMAND SCREENING

RECORDS CHECKED: DDAGERS HEALTH RECORD UNIT PAYMENT LOG

RECORDS SCREENED BY THE COMMAND REFLECT (Check appropriate boxes):

NO DEROGATORY INFORMATION FOLLOWING INFORMATION:

RETURN RESULTS TO:
 SECURITY MANAGER
 HQ, 4TH MARINE REGT.
 CAMP SCHAB

Figure 23-2. Sample Local Records Check For Marines

SOP FOR IPSP



UNITED STATES MARINE CORPS
 HEADQUARTERS BATTALION
 3D MARINE DIVISION (1) (SEINF), FLEET MARINE FORCE
 50TH DEBAR
 PFC AF 8006-8000

DO NOT WRITE IN THESE SPACES

LOCAL RECORDS CHECK (1800)
 NAVMC 10441 (Rev. 3-75), (Previous edition will be void)
 DA FORM 10441-102 (11) 54

DATE _____

NAME (Last, First, Middle) SMITH, John Doe		UIC 123 45 6789	GRADE HM2	BOC
ORGANIZATION HQCo, 4th Marine Regt.				
DATE OF BIRTH 651010	PLACE OF BIRTH Minneapolis, Minnesota			CITIZENSHIP U.S.
NAME OF SPOUSE (Last, First, Middle)	DATE OF BIRTH	PLACE OF BIRTH		CITIZENSHIP
CLEARANCE STATUS (Duty)	BASIS	COMPLETED BY (Agency)		DATE COMPLETED

PURPOSE FOR REQUESTING LOCAL RECORDS CHECK _____

RESULTS OF COMMAND SCREENING

RECORDS CHECKED DOR/SRS HEALTH RECORD UNIT PUNISHMENT LOG

RECORDS SCREENED BY THE COMMAND REFLECT (Check appropriate box):

NO DEGRADATORY INFORMATION FOLLOWING INFORMATION:

RETURN RESULTS TO:
 DIVISION SURGEON'S OFFICE
 3D MARINE DIVISION
 BLDG 4433
 CAMP COURTNEY

Figure 23-3. Sample Local Records Check For Sailors

SOP FOR IPSP

HEADING

5520
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Navy Personnel Officer, 3d Marine Division (DivSurg)
Subj: REQUEST FOR SECRET SECURITY CLEARANCE CASE OF HM2 SMITH,
J. D. 123 45 6789/USN
Ref: (a) OPNAVINST 5510.1_
(b) DivO P5510.9_

1. Per the references, a secret security clearance is requested for SNM. The following information is submitted.

a. Secret eligibility and U.S. citizenship confirmed 920815 with Navy Personnel Office.

b. Local records checks (NAVMC 10482) forwarded to PMO MCB, Butler and (appropriate medical/dental facility on 920815.

SIGNATURE

Copy to:
Security Files

DATE

FIRST ENDORSEMENT

From: Navy Personnel Officer
To: Commanding Officer, (Unit)

Encl: (1) LRC PMO
(2) LRC Medical/dental

1. The enclosures are returned.

SIGNATURE

Figure 23-4. Sample Letter To Navy Personnel Office Requesting Security Clearance

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: EXTENDED INTERIM CLEARANCE AND ACCESS CASE OF SSGT JONES,
J. J. 123 45 6789/0311 USMC

Ref: (a) OPNAVINST 5510.1_
(b) DivO P5510.9_

1. Per the references, an extended interim (level) security clearance and access is granted for a period of 180 days.
2. The previous interim (level) security clearance issued (date) is canceled.
3. This interim (level) security clearance expires on (date).

SIGNATURE

Copy to:
SNM
CMCC
Security Files

Figure 23-5. Sample Letter For Extended Interim Clearance And Access

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: ADMINISTRATIVE REDUCTION OF INTERIM TOP SECRET CLEARANCE
AND ACCESS CASE OF SSGT JONES, J. J. 123 45 6789/0311 USMC

Ref: (a) OPNAVINST 5510.1_
(b) DivO P5510.9_

1. Per the references, an interim top secret security clearance and access has been reduced to secret for failure to submit the required investigation/PR.
2. The interim top secret security clearance issued (date) is canceled.

SIGNATURE

Copy to:
SNM
CMCC
Security Files

Figure 23-6. Sample Letter For Administrative Reduction Of Interim Top Secret Clearance To Secret

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: FINAL (LEVEL) CLEARANCE AND ACCESS CASE OF SSGT JONES,
J. J. 123 45 6789/0311 USMC

REF: (a) SSO Letter dtd/MMS DFR dtd/MISSO Roster dtd (b)
OPNAVINST 5510.1
(c) DivO P5510.9_

1. Per the references, a final (level) security clearance was issued to SNM by DON CAF/COMNAVINTCOM/COMNAVSECGRU on (date).
2. The interim (level) security clearance issued (date) is canceled.

SIGNATURE

Copy to:
SNM
CMCC
Security Files

Figure 23-7. Sample Letter For Final Clearance And Access

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: SPECIAL ACCESS PROGRAM FINAL (LEVEL) CLEARANCE AND ACCESS
CASE OF SSGT JONES, J. J. 123 45 6789/0311 USMC

Ref: (a) OPNAVINST 5510.1_
(b) DivO P5510.9
(c) Applicable Directive(s)

1. Per the references, a final (level) security clearance and access has been granted to SNM due to (Program Name) Special Access Program requirements.

2. All Special Access Program briefing requirements identified in the references have been met and recorded.

SIGNATURE

Copy to:
SNM
CMCC
Security Files
Program Manager if applicable

Figure 23-8. Sample Letter For Final Clearance And Access For Special Access Program

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Special Security Office
To: Commanding Officer, Unit

Subj: FAVORABLE ELIGIBILITY DETERMINATION FOR SCI ACCESS CASE OF
RANK, NAME, INITIALS, SSN/MOS

Ref: (a) SSO Navy msg dtg 010001Z Jan 93
(b) OPNAVINST 5510.1H
(c) DivO P5510.9K

1. Per reference (a), a favorable eligibility determination for SCI access has been made by COMNAVINTCOM/COMNAVSECGRU in the case of SNO/SNM. SNO/SNM has been issued a final top secret security clearance by COMNAVINTCOM/COMNAVSECGRU dated (Date).
2. Using this letter as a reference, you are authorized to grant top secret access to SNO/SNM per the instructions contained in references (b) and (c).
3. This letter will be maintained in SNO's/SNM's security files.
(Include the following as paragraph 4 if applicable)
4. SNO/SNM's final top secret clearance is based on an SBI/SSBI completed (Date). An SSBI Periodic Review (PR) will be submitted to this office no later than (Date). SNO/SNM should contact the unit security manager for assistance with PR submission.

SIGNATURE

Copy to:
Div SecMgr
SSO Files

Figure 23-9. Sample Letter Favorable Eligibility
Determination for SCI Access

SOP FOR IPSP

CHAPTER 24

ACCESS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.....	24000	24-3
REQUEST FOR ACCESS.....	24001	24-3
GRANTING ACCESS.....	24002	24-3
RECORDING ACCESS.....	24003	24-4
ACCESS FOR PERSONNEL ASSIGNED TO TEMPORARY ADDITIONAL DUTY OR ATTACHED FOR DUTY.....	24004	24-4
ACCESS FOR PERSONNEL OF UNIT DEPLOYMENT PROGRAM UNITS.....	24005	24-5
OTHER TYPES OF ACCESS.....	24006	24-5

FIGURE

24-1	SAMPLE CLEARANCE CERTIFICATION LETTER.....	24-7
24-2	SAMPLE LETTER FOR GRANTING ACCESS.....	24-8

SOP FOR IPSP

CHAPTER 24

ACCESS

24000. BASIC POLICY. Access is the opportunity or ability to obtain classified information. Access to classified information, orally, in writing, or by any other means, shall be limited to those whose duties require knowledge or possession thereof. No member of the 3d Marine Division has the right of access to classified information simply by virtue of rank, position or security clearance.

1. The individual who has possession, knowledge, or control of classified information, is responsible for controlling access to it. Before allowing anyone else access to the information, the individual possessing it "must" determine that the other person's official duties justify their being given access to the information (i.e., the "Need-to-Know") and that he/she also has the appropriate security clearance and access authorization from proper authority. For the 3d Marine Division, access authorization officials are the commanding officers of regiments, groups (i.e., CSG) and battalions.

2. Commanding officers will ensure that prior to granting access to classified information, all personnel have executed a Classified Information Nondisclosure Agreement (SF 312) addressed in detail in chapter 24 of reference (c) and chapter 23 of this Order. As stated in paragraph 24-2.3 of reference (c), refusal to sign an SF 312 will cause the command to immediately deny the individual access to classified information, terminate any current access, and inform DON CAF. DON CAF will initiate action to deny or revoke the individual's security clearance.

3. Commanding officers will ensure that prior to granting access, personnel under their jurisdiction are briefed per chapter 3 of reference (c) and this Order.

24001. REQUEST FOR ACCESS. A request for clearance and access to classified information will be submitted to the appropriate commanding officer, per the instructions contained in paragraph 23002 of this Order.

24002. GRANTING ACCESS

1. The ultimate authority for granting access to classified information rests with the commanding officers identified in paragraph 24000.1, who are responsible for the security of the information or material in their command. These commanding officers may grant access to classified information to an individual who has an official "Need-to-Know", a valid security clearance or access authorization, and about whom there is no locally available disqualifying information.

2. A security clearance may be authorized only for the level of access required to perform assigned duties. The clearance

authorization by DON CAF, COMNAVINTCOM or COMNAVSECGRU and the access granted by the command must be at the same level.

3. The authority of commanding officers to grant access to classified information is subject to the restrictions listed in paragraph 24-3.3 of reference (c). Commanding officers will ensure that work section supervisors are made aware of these restrictions, including the restriction to limit access to classified information, when feasible, for those individuals with interim clearances.

4. Since granting access is a command responsibility, access is automatically withdrawn when the individual transfers from the command, is discharged or separated from Federal service.

24003. RECORDING ACCESS

1. The access granted to an individual by a command must be recorded and maintained by the unit security manager. For the 3d Marine Division, figures identified in chapter 23 of this Order serve this purpose.

2. Access granted to the commanding officer need not be recorded, unless it involves special access programs addressed in chapter 23 of reference (c) and paragraph 23005 of this Order.

3. The commanding officer or security manager is responsible for notifying an individual's supervisor when access to classified information has been granted, with specific instructions on any restrictions or limits to access.

24004. ACCESS FOR PERSONNEL ASSIGNED TO TEMPORARY ADDITIONAL DUTY (TAD) OR ATTACHED FOR DUTY

1. When personnel are assigned TAD or attached for duty, and access to classified information will be required; commanding officers will ensure that the individual's level of security clearance is included in the TAD orders, or a clearance certification message or letter is forwarded to the command.

Examples:

a. Members of 7th Communications Battalion are sent TAD to work in the 3d Marine Division Communications Center.

b. Members of 12th Marine Regiment are attached to Headquarters Battalion to work in the Fire Support Coordination Center of the G-3.

2. At the TAD site, the individual will ensure that their orders are presented to the commanding officer or security manager and a request for access to classified information is granted by that command.

3. For personnel assigned TAD to a unit of the 3d Marine Division, the work section to which the individual is assigned will submit a

request for access to classified information, to the commanding officer per paragraphs 24001 and 23002 of this Order. A copy of the individual's TAD orders will be attached to the request. If the individual's security clearance information was forwarded by clearance certification message or letter (figure 24-1), a copy of the message or letter will be attached to the access request.

4. Commanding officers will grant access to classified information for personnel attached for duty or TAD to the unit using figure 24-2.

5. Commanding officers will ensure that attached for duty/TAD personnel are briefed per chapter 3 of reference (c) prior to granting access.

24005. ACCESS FOR MEMBERS OF UNIT DEPLOYMENT PROGRAM (UDP) UNITS

1. Commanding officers of UDP units will submit a clearance certification message or letter to appropriate command elements (i.e., battalion, regiment, division).

2. The clearance certification message or letter will identify individuals of the unit who in the performance of their official duties, will require access to classified information when attending briefings, meetings or planning conferences during the deployment. Specific sections that should receive a copy of the certification message or letter should be identified.

3. The commanding officer or security manager responsible for the security of classified information for the command element, will grant access locally as required, and ensure appropriate distribution of the clearance certification message or letter.

24006. OTHER TYPES OF ACCESS

1. Chapter 24 of reference (c) outlines requirements, restrictions and responsibilities for granting access to classified information for individuals and specific situations listed below.

- a. Temporary access.
- b. One-time access.
- c. Limited access authorization (LAA).
- d. Access by retired personnel.
- e. Access by reserve personnel.
- f. Access by persons outside of the executive branch of government.
- g. Access by former presidential appointees.

h. Access by investigative and law enforcement agents.

2. Under no circumstances will commanding officers grant access to classified information, for these individuals or situations, without first ensuring that the individual or situation meets the criteria and restrictions outlined in chapter 24 of reference (c).

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

FROM: Commanding Officer, (Unit)
To: Assistant Chief of Staff, G-3, 3d Marine Division
Via: Commanding Officer, Headquarters Battalion (SecMgr)

Subj: CLEARANCE CERTIFICATION CASE OF MAJOR I. B. HIPSHOT
123456789/0802 USMC

Ref: (a) OPNAVINST 5510.1
(b) DivO P5510.9

1. Per the references, SNO was issued a top secret clearance on (Date) by DON CAF. SNO will be attached to the Division G-3 to perform duties as a Fire Support Coordination Center Officer. This attachment will be effective for 12 months from the date of this letter.

2. Grant access locally as required.

SIGNATURE

Copy to:
Files
SecMgr

SOP FOR IPSP

HEADING

5510
ID SYMBOL
DATE

From: Commanding Officer/Security Manager
To: Work section

Subj: ACCESS GRANTED TO (LEVEL) INFORMATION CASE OF SSGT JONES,
J. J. 123 45 6789/0311 USMC

Ref: (a) Clearance certification message/Orders
(b) OPNAVINST 5510.1H
(c) DivO P5510.9K

1. Per the references, SNM has been granted (level) access to classified material while performing duties with this unit in a Temporary Additional Duty (TAD) status.

2. This access authorization will remain in effect until SNM is detached, or until access to classified information is no longer required to perform his official duties.

SIGNATURE

Copy to:
SNM
CMCC
Security Files

Figure 24-2. Sample Letter For Granting Access

SOP FOR IPSP

APPENDIX A

REFERENCES

- (a) DOD 5200.1-R, Department of Defense Information Security Program Regulation
- (b) DOD 5200.5200.2-R, Department of Defense Personnel Security Program Regulation
- (c) OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation
- (d) CSP 1A, Cryptographic Security Policy and Procedures (U)
- (e) CMS 4L, Communication Security Material System (CMS) Manual
- (f) MCO 5510.7F, Marine Corps Personnel Reliability Program (PRP)
- (g) FMFPacO P03401.7C (C), Nuclear Weapons Management Manual (U)
- (h) NWP (O), Naval Warfare Documentation Guide
- (i) TRI-MEF P2000.2, Comm and Computer System SOP
- (j) ForO 5239.1, Automated Data Processing (ADP) Security Procedures
- (k) DivO P5230.1, SOP for End User Computer
- (l) MCO 2201.1, Communications Security (COMSEC)
- (m) DivO P2000.10C, SOP for Communications - Electronics
- (n) FMFPacO 3070.1A, Operations Security
- (o) ForO 3100.1B, Operations Security
- (p) MCO 2021.1, Operation and Management of Marine Corps World Wide Military Command and Control System (WWMCCS) Intercomputer Network Remote Terminal Sites
- (q) JCS Pub 6-03.7, Security Policy for the WWMCCS Intercomputer Network
- (r) ForO 5210.1A, Desktop Procedures and Turnover Folders
- (s) DivO 5040.3C, SOP for Command Readiness Evaluation Program
- (t) JAGINST 5800.7, Manual of the Judge Advocate General
- (u) DivO P2110.1E, SOP for Message Handling and Preparation

SOP FOR IPSP

- (v) CNO ltr 2220 Ser 09N2/9U651988 dtd 1 Aug 1988
- (w) USFJ Policy ltr 205-1 dtd 9 Nov 90
- (x) DOD Directive TS-5105.21-M-2
- (y) Navy Supplement to DOD C-5105.21-M-1
- (z) MCO P1070.12H, Marine Corps Individual Records Administrative Manual (IRAM)
- (aa) MCO P1080.35H, Personnel Reporting Instructions Manual (PRIM)
- (bb) MCO 5521.3H, Personnel Security Investigations, Security Clearances, and Access
- (cc) MCO P1080.20K, Joint Uniform Military Pay System/Manpower Management System Codes Manual
(Short title: JUMPS/MMSCODESMAN)