

MARFORPACO P5510.18



STANDING OPERATING PROCEDURES

FOR THE INFORMATION AND

PERSONNEL SECURITY PROGRAM

UNITED STATES MARINE CORPS
Headquarters, Marine Forces Pacific
Camp H. M. Smith, HI 96861-5001

MARFORPACO P5510.18
02/SecMgr/B-11A
18 Sep 1995

MARINE FORCES PACIFIC ORDER P5510.18

From: Commander
To: Distribution List

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

Ref: (a) OPNAVINST 5510.1H
(b) SECNAVINST 5720.42E
(c) MCO 5510.9A
(d) MCO 5521.3H

Encl: (1) LOCATOR SHEET

1. Purpose. To publish standing operating procedures (SOP) for the information and personnel security program within this headquarters per references (a) through (d).
2. Action. Addressees will implement the information and personnel security procedures and measures set forth herein. Division and separate branch heads and the Commanding Officer, Headquarters and Service Battalion (CO HQSVCBn) are encouraged to establish internal written security procedures to implement regulations within this Manual for offices under their cognizance.
3. Certification. Reviewed and approved this date.


W. P. ARMES
Chief of Staff

DISTRIBUTION: LIST I A

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

Location:

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

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CONTENTS

CHAPTER

- 1 INTRODUCTION TO THE INFORMATION AND PERSONNEL
SECURITY PROGRAM
- 2 PROGRAM MANAGEMENT
- 3 SECURITY EDUCATION
- 4 COMPROMISE AND OTHER SECURITY VIOLATIONS
- 5 COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO
THE SECURITY MANAGER
- 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 MATERIAL
- 18 VISITOR CONTROL
- 19 MEETINGS
- 20 PERSONNEL SECURITY POLICY
- 21 PERSONNEL SECURITY INVESTIGATIONS

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

22	PERSONNEL SECURITY DETERMINATIONS
23	CLEARANCE
24	ACCESS

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	1000	1-3
RESPONSIBILITIES	1001	1-3
SPECIAL ACCESS PROGRAMS.	1002	1-3
SENSITIVE COMPARTMENTED INFORMATION.	1003	1-4
ATOMIC ENERGY ACT.	1004	1-4

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

1000. BASIC POLICY. The Department of the Navy (DON) Information and Personnel Security Program Regulation (current edition of OPNAVINST 5510.1) provides the basic guidance for the security of classified information and personnel security matters.

1001. RESPONSIBILITIES

1. Each person who handles classified material and information is responsible for safeguarding it and is responsible individually for compliance with this Manual in all respects.

2. In addition to individual responsibility, procedures for the protection and control of classified material and information will be established in each office space containing classified material.

3. Overall responsibility for classified material and information within each division and section rests with the designated division and section head.

4. The policies and procedures in this Manual represent the minimum requirements for the handling, control, accountability and storage of classified information within this headquarters. Division and branch heads and special staff officers may choose to impose more stringent requirements within areas under their cognizance. They may not establish requirements that impact on others or are contrary to the contents of this Manual.

5. Individual requests for guidance and interpretation of this Manual are encouraged. All such requests should be addressed to the Security Manager (Assistant Chief of Staff, G-1 (AC/S G-1)).

6. Security Manager Notes are issued periodically by the Security Manager (AC/S G-1). Security Manager Notes are not directives but reflect official interpretation of security policies and procedures and provide information concerning pending changes in the Information and Personnel Security Program.

1002. SPECIAL ACCESS PROGRAMS. Special access programs identified in the current edition of OPNAVINST 5510.1 are controlled in this headquarters by the AC/S G-2 and the AC/S G-3. With the exception

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

of these special access programs, no other special access programs will be implemented within this headquarters without the approval of the Security Manager.

1003. SENSITIVE COMPARTMENTED INFORMATION. All Sensitive Compartmented Information (SCI) or Special Intelligence (SI) material received by this headquarters will be handled and controlled, per established regulations, by the Special Security Office/Special Activities Office (SSO/SAO). Access to this information will also be controlled by the SSO/SAO.

1004. ATOMIC ENERGY ACT. The Atomic Energy Act of 30 August 1954, as amended, and the Department of Energy Directives regulate the handling, protection and classification of Restricted Data and Formerly Restricted Data. The current edition of OPNAVINST 5510.1 provides for the handling of this information.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 2
PROGRAM MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	2000	2-3
DESIGNATION AND RESPONSIBILITIES.	2001	2-3
INTERNAL SECURITY PROCEDURES.	2002	2-9

FIGURE

2-1	SAMPLE LETTER OF APPOINTMENT FOR SECONDARY CONTROL POINT CUSTODIAN/ALTERNATE . .	2-11
2-2	SAMPLE LETTER OF INVENTORY/RELIEF OF CUSTODIAN OR SECONDARY CONTROL POINT.	2-12

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 2

PROGRAM MANAGEMENT

2000. BASIC POLICY. The Commander, Marine Forces Pacific (COMMARFORPAC) is ultimately responsible for all classified material received for or originated by this headquarters.

2001. DESIGNATION AND RESPONSIBILITIES. In order to facilitate proper handling and safeguarding of these materials within this headquarters, the following controls have been established:

1. Security Manager

a. The Assistant Chief of Staff, G-1 (AC/S G-1) is the MARFORPAC Security Manager.

b. The Security Manager coordinates the total security control program within this headquarters for classified material and information.

2. Security Assistants

a. Each division, branch or special staff section that is authorized to receipt for and store classified material will appoint in writing, a security assistant. A copy of the appointment letter will be forwarded to the Security Manager to facilitate the coordinator of information and personnel security matters. Security assistants are responsible to the division and branch heads for internal security of classified material within the section. The security assistant should be an individual senior enough to exercise authority to manage the information and personnel security program within a respective section. Security assistants are encouraged to maintain liaison with the MARFORPAC Security Manager relative to security matters.

b. Section Responsibilities

(1) The G-2 Division will manage, advise and assist the security manager on counterintelligence matters, special access programs and management of the special security officer functions.

(2) The G-3 Division will manage, advise and assist the security manager on operations security (OPSEC).

(3) The G-4 Division will manage, advise and assist the security manager on security equipment procurement matters.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

(4) The G-6 Division will manage, advise and assist the security manager on automated data processing, communications security and Worldwide Military Command and Control System (WWMCCS).

(5) The MARFORPAC Public Affairs Officer (PAO) will advise and assist the security manager on security review before public release of briefs and articles.

(6) The Provost Marshall Office (PMO) will advise and assist the security manager on physical security, theft prevention and anti-terrorism.

(7) The Classified Material Control Center (CMCC) will manage, advise and assist the security manager on document security administration and document control.

(8) The MARFORPAC Adjutant, working under the guidance of the G-1 Division, will advise and assist the security manager on visitor control in conjunction with the MARFORPAC Protocol Officer. The Force Adjutant will also be assigned as the officer-in-charge (OIC) of the CMCC.

(9) Headquarters and Service Battalion (HQSVCBn) will manage the administration of personnel security clearances and accesses.

3. Officer-in-Charge, Classified Material Control Center (CMCC)

a. The Officer-in-Charge (OIC), CMCC receives, processes and maintains required accountability for all classified material received, originated, maintained or mailed by this headquarters.

b. Staff cognizance is provided by the Force Adjutant who will assign an officer the duties of OIC CMCC and additional duties as the MARFORPAC Top Secret Control Officer (TSCO).

c. The OIC CMCC/TSCO will be appointed in writing by the COMMARFORPAC. A copy of the appointment letter will be forwarded to the Security Manager.

4. Top Secret Control Officer

a. The Top Secret Control Officer is responsible for all Top Secret material received or originated by this headquarters, with the exception of SCI material which is controlled by the SSO. The TSCO is an additional duty of the OIC CMCC. Secret material will be controlled per the provisions of the current edition of OPNAVINST 5510.1 and this Manual.

b. The duties of the Top Secret Control Officer will be assigned to a Gunnery Sergeant or above. Exception to policy will be requested through the Security Manager, MARFORPAC, with full justification for a waiver request. The Top Secret Control Officer will be appointed in writing by the COMMARFORPAC.

c. The Top Secret Control Officer is responsible to the Security Manager for the receipt, custody, control, accountability and disposition of Top Secret material in this headquarters.

5. Assistant Top Secret Control Officer

a. An Assistant Top Secret Control Officer will be appointed in writing by the COMMARFORPAC to assist the Top Secret Control Officer in the performance of duty. A copy of the appointment letter will be forwarded to the Security Manager.

b. The duties of the Assistant Top Secret Control Officer will be assigned to a Staff Sergeant or above.

c. The Assistant Top Secret Control Officer is responsible to the Top Secret Control Officer, and will assist in the accountability and control of Top Secret material.

6. Top Secret Control Assistants

a. Each division, branch or special staff section authorized to receive, store or process Top Secret material will designate a Top Secret Control Assistant. The Top Secret Control Assistant will be responsible for all Top Secret material originated, stored, received or processed by their respective section.

b. The duties of the Top Secret Control Assistant will be assigned in writing to a Staff Sergeant or above. Requests for exceptions to the grade requirements will be addressed to the Security Manager.

c. The Top Secret Control Assistants are responsible to the MARFORPAC Top Secret Control Officer.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM7. Secondary Control Point (SCP) Custodian

a. When an SCP has been authorized to be established at a division/branch, an SCP custodian, a Staff Sergeant or above, and an alternate, Corporal or above, will be appointed in writing by the division or branch head. Figure 2-1 is a sample format for the appointment letter. A copy of the appointment letter will be retained by CMCC, SCP and the MARFORPAC Security Manager. Requests for exception to the grade requirements will be addressed to the Security Manager with full justification for subject waiver.

b. Prior to changing the SCP custodian or alternate, an inventory of all classified material will be conducted and the results forwarded to the OIC CMCC. A record of this inventory will be maintained at the SCP for two years. Figure 2-2 is a sample format of the inventory letter. Discrepancies will be reported to the Security Manager for appropriate action.

c. The SCP custodian, or in their absence, the SCP alternate, is the division or branch head's representative responsible for implementing and maintaining required controls of all classified material held or circulated by the division or section SCP. This includes:

- (1) Receipt.
- (2) Routing.
- (3) Maintenance of up-to-date records of materials held.
- (4) Records of destruction.
- (5) Ensuring that only authorized persons have access to classified material.
- (6) Promulgation and periodic review of policy and procedures for the control of classified material within the SCP of divisions and sections.

8. Automated Data Processing (ADP) Security Officer

a. The ADP Security Officer is responsible for the security of classified information processed in the Systems Integration HUB (SIH) and is the command's representative for ADP security matters.

b. Staff cognizance for the ADP Security Officer is provided by the AC/S G-6. The duties of the ADP Security Officer will be assigned to an individual, Staff Sergeant or above.

c. The ADP Security Officer is responsible to the Security

Manager for the protection of classified information being processed by the SIH.

9. Communications Security (COMSEC) Officer

a. The COMSEC Officer is responsible for ensuring the security of military communications within this headquarters and throughout MARFORPAC.

b. Staff cognizance for the COMSEC Officer is provided by the AC/S G-6 who will assign an individual as the MARFORPAC COMSEC Officer. The COMSEC Officer within this headquarters will be guided in the performance of duties by the current edition of MARFORPACO 02230.1 and will be appointed in writing by the Communication-Electronics Officer (AC/S G-6) (assigned by T/O billet/line number (4929N/202)).

10. Special Security Officer/Special Activities Officer

a. Within this headquarters, the SSO/SAO is responsible for the Sensitive Compartmented Information Facility (SCIF) and the security, control, dissemination and use of all SCI and Special Intelligence (SI) material. The SSO/SAO is also responsible for personnel security associated with this type of material.

b. The AC/S G-2 will assign the SSO in writing.

c. The SSO can be the Security Manager; however, the Security Manager must meet the requirements for SCI access and be designated as the SSO by the Commander, Naval Intelligence Command or Commander, Naval Security Group.

11. Operations Security (OPSEC) Officer

a. The OPSEC Officer is responsible for ensuring security of military operations within this headquarters.

b. Staff cognizance for OPSEC is provided by the AC/S G-3 who will assign an individual (in writing) as the MARFORPAC OPSEC Officer.

12. North Atlantic Treaty Organization (NATO) Control Officer. The NATO Control Officer is responsible for all matters relating to NATO material and will be guided in the performance of duties by the current edition of OPNAVINST C5510.101. The NATO Control Officer will be appointed in writing by MARFORPAC Special Order.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM13. COMSEC Material System Custodian (CMS)

a. The CMS custodian within this headquarters will be guided in the performance of duties by the current edition of CMS 1 and will be appointed in writing by MARFORPAC Special Order.

b. The CMS custodian will not be assigned duties as the Naval Warfare Publications Library (NWPL) Custodian.

14. Naval Warfare Publications Library (NWPL) Custodian

a. The NWPL Custodian will be designated in writing by MARFORPAC Special Order and act as the central control point for the handling and distribution of NWP within this headquarters. The responsibility of coordinating the tactical improvement program, to include the review of NWPs, rests with the AC/S G-3.

b. The NWPL custodian will be guided in the performance of duties by the current edition of NWP 1-01

c. The NWPL Custodian will not be assigned duties as the CMS Custodian.

d. The NWPL Custodian is responsible to the Security Manager for accountability and control of NWPs.

15. Classified Material Control Center (CMCC)

a. The CMCC houses the command's classified files and related control records.

b. The CMCC is the primary control center for all classified matter addressed to or originated by this headquarters.

16. Secondary Control Points (SCPs)

a. SCPs are administrative security storage areas at division and section levels which assist in the control of classified matter.

b. All SCPs will be inspected and authorized in writing by the MARFORPAC Security Manager prior to the storage of classified material within the respective division and section.

17. Emergency Action Plans (EAPs)

a. The OIC CMCC will develop emergency action plans for the handling and control of classified material within this headquarters during emergency periods. Paragraph 17005 of this Manual provides detailed guidance regarding emergency destruction

of classified material.

b. Each division and section within MARFORPAC that has been authorized a SCP, will develop an EAP for the handling and control of classified material in the event of an emergency. This EAP will be maintained on file within the confines of that section.

c. Prior to finalizing an EAP, the proposed EAP will be provided to CMCC for approval.

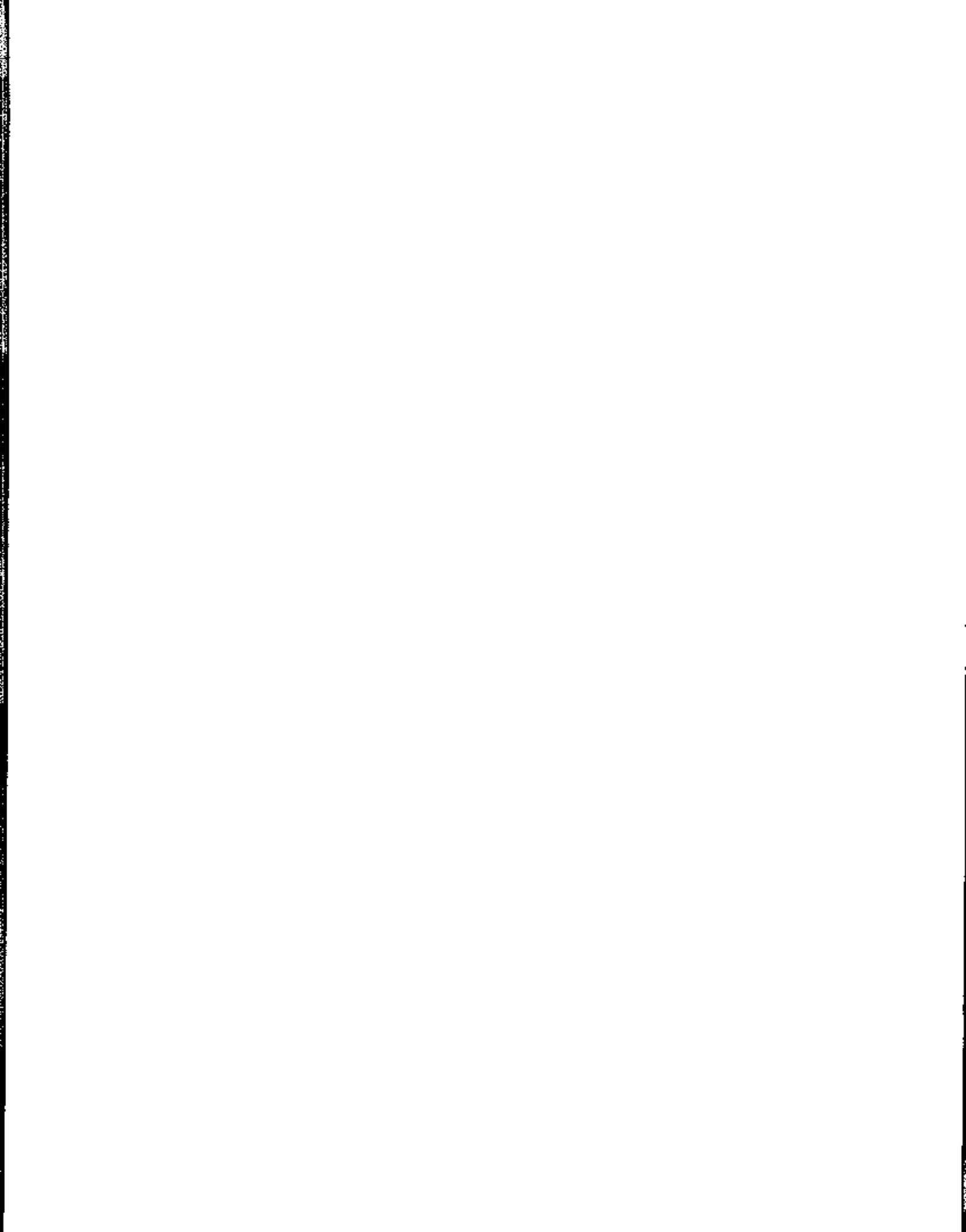
d. Once approved, a copy of the EAP will be forwarded to the OIC CMCC for formulation of the MARFORPAC EAP in coordination with the Security Manager and the CO HQSVCBn, Camp H. M. Smith.

2002. INTERNAL SECURITY PROCEDURES

1. Each division, branch and special staff section which handles classified information is required to prepare and keep current, written security procedures specifying how the requirements of this Manual will be accomplished within their specific offices.

2. Internal security procedures should include, but are not limited to, accounting and control of classified material, physical security measures for protecting it, control of reproduction, destruction, screening of incoming material until a security determination has been made, requesting and recording clearance and access, security education, review of classified material for proper classification and marking, downgrading and declassification, and the control of visitors.

3. Internal security procedures should cover what is to be done, who is to do it and who is to supervise. General statements such as "handle SECRET material per the current edition of MARFORPACO P5510.18" are not considered adequate for internal security procedures.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

HEADING

5510
(Originator)
(Date)

From: (Head, Division/Section/Activity)
To: Officer in Charge, Classified Material Control Center
Via: Assistant Chief of Staff, G-1, Security Manager

Subj: APPOINTMENT OF SECONDARY CONTROL POINT CUSTODIANS

Ref: (a) MARFORPACO P5510.18

1. The below listed individuals are appointed as Secondary Control Point Custodians and Alternates for (Section) per the provisions of paragraph 2001.6 of the reference. These individuals are authorized to receipt for classified material up to and including (level).

SECONDARY CONTROL POINT CUSTODIAN

PRIMARY

NAME	GRADE	SSN	SECTION	SIGNATURE
------	-------	-----	---------	-----------

ALTERNATE

NAME	GRADE	SSN	SECTION	SIGNATURE
------	-------	-----	---------	-----------

2. Point of contact is LtCol I. M. InCharge.

I. M. INCHARGE

Copy to:
Officer/Enlisted concerned

Figure 2-1.--Sample Letter of Appointment for Secondary Control Point Custodian/Alternate.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

HEADING

5510
(Originator)
(Date)

From: Secondary Control Point Custodian, (Section/Branch)
To: Officer in Charge, Classified Material Control Center
Subj: INVENTORY/RELIEF OF SECONDARY CONTROL POINT CUSTODIAN
Ref: (a) MARFORPACO P5510.18

1. Per the reference, the subject inventory was conducted on (date) and held in conjunction with change of custodian inventory.
2. All classified material on charge to this (division or branch) was accounted for.
3. *The below listed discrepancy(ies) were noted:

Signature

Copy to:

*As required

Figure 2-2.--Sample Letter of Inventory/Relief of Custodian of
Secondary Control Point.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 3

SECURITY EDUCATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC GUIDANCE	3000	3-3
PURPOSE OF THE SECURITY EDUCATION PROGRAM.	3001	3-3
RESPONSIBILITY	3002	3-3
SCOPE OF THE SECURITY EDUCATION PROGRAM.	3003	3-4
MINIMUM REQUIREMENTS	3004	3-4
TYPE OF SECURITY BRIEFINGS	3005	3-5
SPECIAL BRIEFINGS.	3006	3-5
DEBRIEFINGS.	3007	3-6
CONTINUING SECURITY AWARENESS.	3008	3-7

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 3

SECURITY EDUCATION

3000. BASIC GUIDANCE. Each command in the DON, which handles classified information, is responsible for establishing and maintaining an active security education program to instruct all personnel, regardless of position or grade, in the command's security policies and procedures.

3001. PURPOSE OF THE SECURITY EDUCATION PROGRAM

1. Basic to a security education program is the appreciation that there is a need for protecting classified information from hostile threats. The purpose of the Information and Personnel Security Program is to provide a framework for the protection of information essential to national security.

2. The purpose of the security education program is to make sure that all personnel understand the need to protect classified information and know how to safeguard it. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties, and the security of classified information becomes a natural element of every task.

3002. RESPONSIBILITY

1. The CO HQSVCBn, as a function of training, is responsible for ensuring that all personnel assigned to the battalion receive a security orientation and indoctrination briefing as soon as possible upon reporting to this headquarters.

2. The Security Manager MARFORPAC is responsible for ensuring that all personnel assigned for duty with MARFORPAC participate in a continuous security education program.

3. Division and separate branch heads are responsible for identifying the security requirements for the functions under their cognizance and for seeing that personnel under their supervision are familiarized with the security requirements for their particular assignments. On-the-job (OJT) training is an essential part of this headquarters' security education program and must be exercised within all offices.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM3003. SCOPE OF THE SECURITY EDUCATION PROGRAM

1. Security education must be provided to all personnel, whether they have access to classified information or not. Obviously, a more extensive security education program must be provided to those individuals who do have access. The MARFORPAC Security Education Program has been developed to meet the needs of this headquarters.

2. The MARFORPAC Security Education Program has been designed to accomplish the following:

a. Advise personnel of the need for protecting classified information, the adverse effects to national security resulting from unauthorized disclosure, and their legal responsibility to protect classified information in their possession.

b. Familiarize personnel with specific security procedures.

c. Familiarize personnel with procedures for challenging classification decisions.

d. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting attempts.

e. Advise supervisors of the requirement of continuous evaluation of personnel for the continuous eligibility for access or assignment to sensitive duties.

f. Advise personnel of the penalties for engaging in espionage.

g. Advise personnel of the hazards involved and the strict prohibition against discussing classified information over the telephone or in any manner susceptible to interception by unauthorized persons.

h. Advise personnel of the disciplinary actions that may result from willful or negligent violation or disregard of the guidance and procedures within this Manual.

3004. MINIMUM REQUIREMENTS. The following are the minimum requirements for security education within this headquarters.

1. Indoctrination in the basic principles of security upon entering the DON.

2. Orientation of those who will have access to classified information at the time of assignment.

3. OJT in specific requirements for the duties assigned.
4. Annual refresher briefings for those who have access to classified information.
5. Special briefings as circumstances dictate.
6. Debriefing at the time a Security Termination Statement is executed. Debriefings are conducted by the CO HQSVCBn.

3005. TYPE OF SECURITY BRIEFINGS. The following are the types of security education presented within this headquarters.

1. Security Orientation and Indoctrination Briefing. A basic indoctrination and orientation to the information and personnel security program within MARFORPAC. This briefing is normally conducted in conjunction with the HQSVCBn Welcome Aboard Brief for all newly assigned personnel 0-3 and below. All field grade personnel will be given an orientation briefing by the Security Manager, on an individual basis, upon assignment to this headquarters.
2. On-the-Job Training. Supervisors must assure themselves that subordinates know the security requirements impacting on the performance of their duties. On-the-job training is that phase of security education that must be a continuous process and constantly evaluated to ensure that the security posture of the office is being maintained per this Manual.
3. Refresher Briefings. Refresher briefings are conducted on an annual basis for all individuals who have been granted access to classified information in this headquarters. Refresher briefings can cover day to day operations of the particular office or the headquarters itself. Refresher briefings can be arranged through the Security Manager or via the HQSVCBn Training Office.
4. Naval Criminal Investigative Service (NCIS) Briefings. Once every two years, all personnel who have access to Secret or above, must be given a counterespionage briefing by the NCIS. These briefings are scheduled twice a year by the Security Manager via the Counterintelligence/HUMINT officer (CIHO).

3006. SPECIAL BRIEFINGS. Certain types of special briefings are required within this headquarters and are coordinated by the Security Manager. These include the following:

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

1. Foreign Travel Briefing. Any individual who has or has had access to classified information, who plans to travel to or through a designated country to attend a meeting in the United States or elsewhere in which representatives of designated countries are expected to participate, must be given a defensive briefing. Cruises on Soviet ships, which have become available recently, also require this precautionary briefing. Foreign travel briefings will be conducted by the Security Manager.

2. NATO Briefings. All personnel who require access to NATO information must be briefed on NATO security procedures by the Security Manager before access is granted. (See the current edition of OPNAVINST C5510.101, for NATO security briefing requirements.)

3. Single-Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI). A special briefing is required before access to SIOP-ESI is granted. The briefing is given by the Security Manager and is based on the current edition of OPNAVINST S5511.35. A briefing (and debriefing) certificate, in the form recommended in the current edition of OPNAVINST S5511.35, must be executed.

4. Sensitive Compartmented Information (SCI). The Special Security Officer (SSO) is responsible for briefing those who are to have access to SCI.

3007. DEBRIEFINGS

1. Those individuals of this headquarters who have had access to classified information, must be debriefed and must execute a Security Termination Statement under the following conditions:

a. 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.

b. At the conclusion of the access period when a Limited Access Authorization has been granted.

c. When security clearance is revoked for cause.

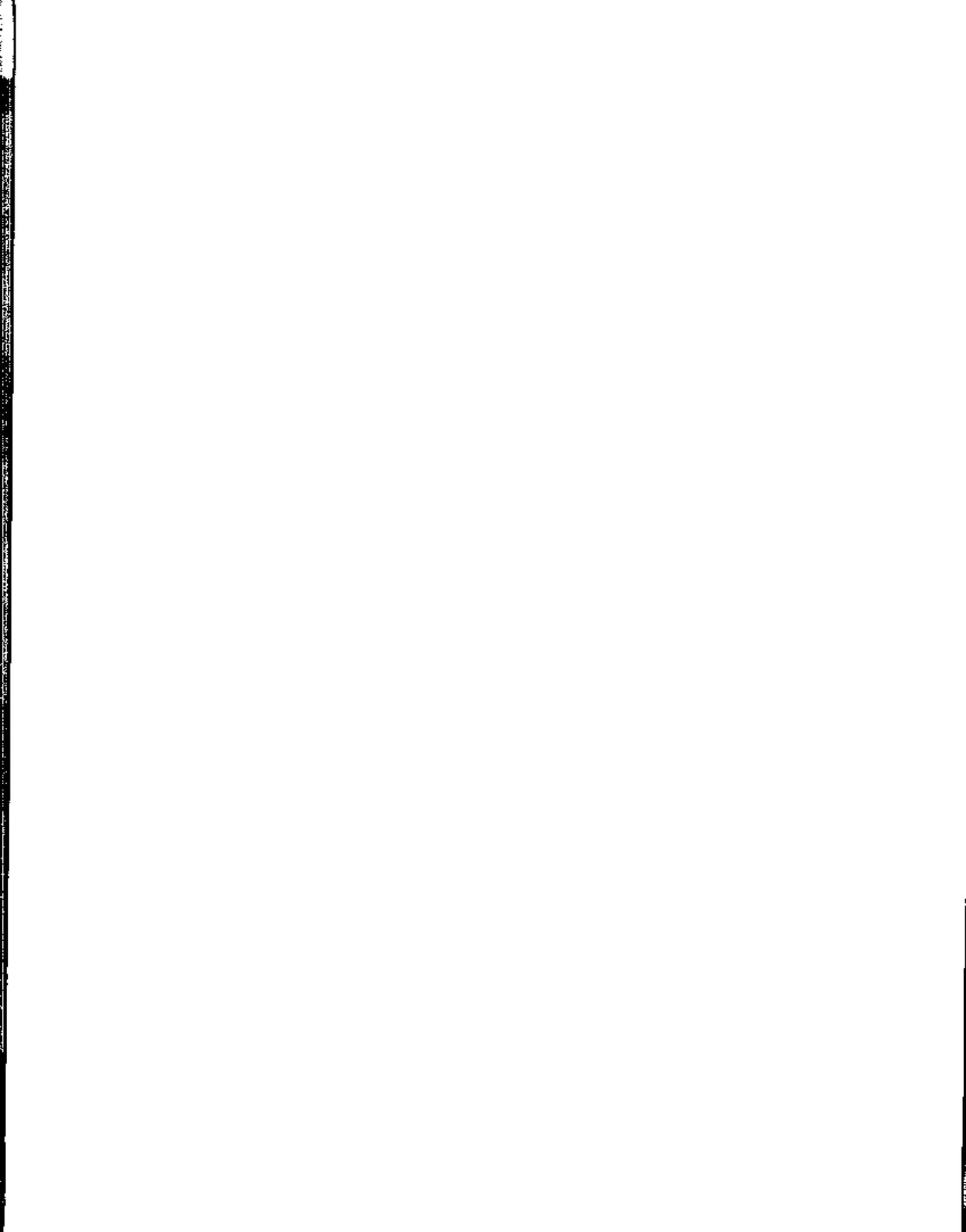
d. When security clearance is administratively withdrawn.

2. A debriefing will also be given and a Security Termination Statement executed, when a member of this headquarters inadvertently has substantive access to information which the member is not eligible to receive.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

3008

3008. CONTINUING SECURITY AWARENESS. The previous paragraphs describe the minimum briefing requirements for the headquarters' security education program. To enhance security in a continuing program, personnel should be frequently exposed to current information. Signs, posters and bulletin board notices are some of the media which should be used to boost security awareness. These materials are available from the Security Manager. Security Manager Notes also help to reinforce the security education program. All requests for security education should be sent to the Security Manager via the HQSVCBn Training Office.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 4

COMPROMISE AND OTHER SECURITY VIOLATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	4000	4-3
ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES AND PUNITIVE ACTIONS	4001	4-3
DISCOVERY OF COMPROMISE OR SUBJECTION TO COMPROMISE.	4002	4-4
PRELIMINARY INQUIRY	4003	4-4
INVESTIGATIVE ASSISTANCE.	4004	4-6
REPORT OF FINDING CLASSIFIED MATERIAL PREVIOUSLY REPORTED AS LOST OR DESTROYED.	4005	4-6
COMPROMISE THROUGH PUBLIC MEDIA	4006	4-6
SECURITY VIOLATIONS	4007	4-6
UNSECURED SECURITY CONTAINERS	4008	4-6
IMPROPER TRANSMISSION	4009	4-7



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 4

COMPROMISE AND OTHER SECURITY VIOLATIONS

4000. BASIC POLICY

1. There are two types of security violations: The first results in the compromise or a possible compromise of classified information. The second occurs when security regulations are violated but there is no compromise of classified material.
2. 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. Compromise is confirmed when conclusive evidence exists that classified information has been disclosed to an unauthorized person. Compromise is possible when some evidence exists that classified information has been subjected to unauthorized disclosure.
3. The 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.
4. Compromise obviously presents the greater threat to national security, but other security violations must also be treated seriously because they demonstrate that a weakness exists in the headquarters' security program. For this reason, security violations of either type must be reported and vigorously investigated and the problems causing the violation corrected rather than covered up. Incidents of an individual's failure to comply with the policies and procedures for safeguarding classified information will be evaluated to determine eligibility to hold a security clearance.

4001. ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES AND PUNITIVE ACTIONS

1. Civilian employees are subject to administrative sanctions, civil remedies and criminal penalties if they knowingly, willfully or negligently disclose classified information to an unauthorized person or knowingly or willfully violate provisions of this Manual for classification and protection of classified information. Sanctions include, but are not limited to, a warning, written notice, reprimand, suspension without pay, forfeiture of pay, removal or discharge.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

2. Military personnel are subject to punitive action, either in civil 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 provisions of this Manual for classification and protection of classified information.

3. Disciplinary action is used primarily to make it clear to the offender, and other personnel, that lax security procedures will not be tolerated. Action taken for involvement in security violations should suit the offense and be applied regardless of grade.

4002. DISCOVERY OF COMPROMISE OR SUBJECTION TO COMPROMISE

1. Any individual who becomes aware of a compromise or subjection to compromise of classified information or material, will immediately notify the most readily available command. The custodian of classified information who causes information to be subjected to compromise, or who becomes aware that information has been subjected to compromise through unauthorized disclosure, abstraction, destruction, loss or theft, must report the subjection to compromise to their superior officer immediately. For incidents of compromise or subjection to compromise within this headquarters, the Security Manager will be immediately notified.

2. The overriding priority is to regain custody of the information, if possible, and give it proper protection. If custody of material believed to be in an area beyond the jurisdiction of the United States cannot be regained, any information identifying the location of the material will be classified at the same level as the unretrieved material.

4003. PRELIMINARY INQUIRY

1. Within this headquarters, a preliminary inquiry will be conducted when classified information is compromised or subjected to compromise. Preliminary inquiries will be conducted by an individual assigned external to the division or branch requiring the inquiry. The Deputy Commander will assign (in writing) an officer to conduct the preliminary inquiry. All preliminary inquiries will be completed within five working days and reported to COMMARFORPAC via the Security Manager. Requests for extensions will be provided to the Deputy Commander via the Security Manager.

2. At a minimum, all preliminary inquiries will include the following information:

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

4003

a. Identify the compromised information completely and accurately. This identification should include the classification of the material, all identification or serial numbers, the date, the originator, the subject, downgrading and declassification instructions and, in the case of documents, the number of pages involved.

b. Determine the circumstances surrounding the incident.

c. Identify all witnesses to the violation and informally interview them to determine the extent of the violation.

d. Identify the individual responsible, if possible.

e. Make an attempt to discover the weaknesses in security procedures that allowed the compromise or subjection to compromise to occur.

f. Evaluate the information compromised or subjected to compromise to determine the extent of potential damage to national security, and the action necessary to minimize the effects of the damage.

g. Establish either:

(1) That an unauthorized disclosure of classified information did not occur or that compromise may have occurred but under conditions presenting a minimal risk to National security.

(2) That compromise is confirmed or that the probability of damage to the national security cannot be discounted.

3. If it is determined that a compromise, or possible compromise in fact did not occur, the preliminary inquiry will still be conducted to determine what security weaknesses existed that permitted the violation to occur.

4. If during the conduct of the preliminary inquiry a determination is made that compromise is confirmed or that probability of damage to National security cannot be discounted, or a significant weakness is revealed, or punitive action is appropriate, a JAG Manual Investigation will be initiated.

5. When COMSEC material has been subjected to compromise, the reporting procedures contained in the current edition of CMS-1 will be used to report the incident. Deviation from these reporting procedures is not authorized.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

4004. INVESTIGATIVE ASSISTANCE. A preliminary inquiry or JAG Investigation may, under certain circumstances, require professional or technical assistance. The individual conducting the inquiry or investigation may seek the assistance of counter-intelligence personnel assigned to the AC/S G-2. All requests for assistance will be forwarded to the Security Manager.

4005. REPORT OF FINDING CLASSIFIED MATERIAL PREVIOUSLY REPORTED AS LOST OR DESTROYED. When classified material previously reported as lost or destroyed is subsequently found, the Security Manager will be notified.

4006. COMPROMISED THROUGH PUBLIC MEDIA. If any member of this headquarters becomes aware that classified information may have been compromised as a result of disclosure in the public media, i.e., newspaper, magazine, radio, or television, the member must notify the Security Manager.

4007. SECURITY VIOLATIONS. Security violations identified during the conduct of Unannounced Counterintelligence Inspections will be reported to COMMARFORPAC. Normally, security violations demonstrate a weakness in the security program. For this purpose, a preliminary inquiry must also be vigorously and thoroughly conducted. This gives division and branches a "second chance" to shore up their security program before a compromise does occur. Paragraph 4003 above provides detailed guidance concerning the conduct of a preliminary inquiry. The possibility of disciplinary or administrative action in a violation that does not include a compromise is just as real as in the case of a violation which leads to a compromise.

4008. UNSECURED SECURITY CONTAINERS. If a container in which classified material is stored is found unlocked in the absence of assigned personnel, report the incident immediately to the Command Duty Officer (CDO). The container will be guarded until the CDO arrives at the location of the unlocked container. The CDO will then inspect the classified material involved, lock the container and notify the Security Manager the following working day. If the CDO believes that the classified information may have been compromised, the CDO will require the person responsible for the container to return to the office to make a complete inventory and will subsequently notify the Security Manager.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

4009

4009. IMPROPER TRANSMISSION. All classified material received at this headquarters is normally processed via the CMCC. However, because Confidential and Secret material can be sent via First Class registered mail, it is possible that divisions and separate branches could receive classified material directly from the mail room. All official mail should be opened immediately upon receipt to ensure that it does not contain classified material. If classified material received shows that it was improperly handled or that it was not properly prepared for transmission, i.e., no inner envelope, no classification marking on the inner envelope, etc., the Security Manager will be notified. The Security Manager will notify the transmitting command.

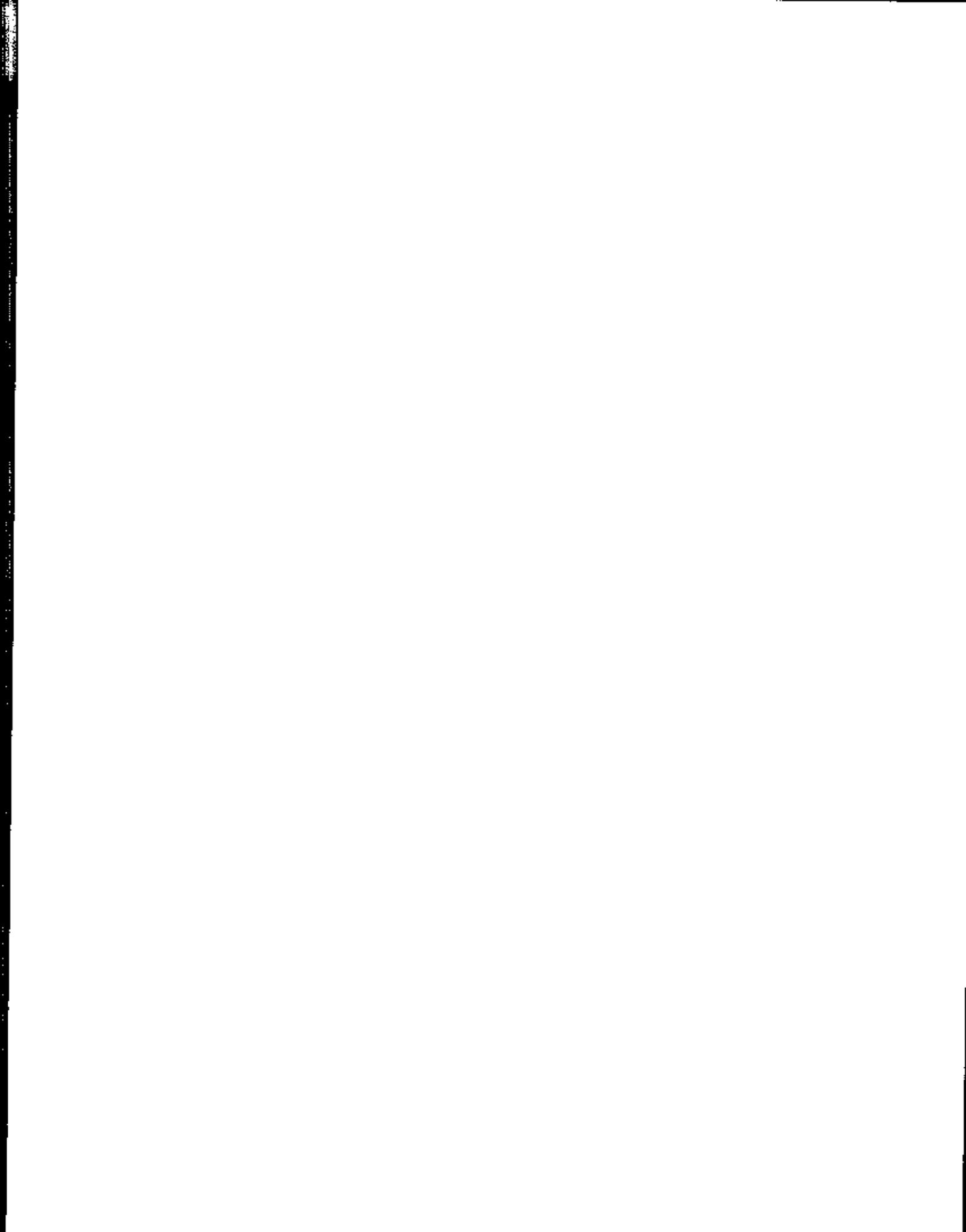


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 5

COUNTERINTELLIGENCE MATTERS TO BE REPORTED
TO THE SECURITY MANAGER

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	5000	5-3
REPORTING RESPONSIBILITIES	5001	5-4



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 5

COUNTERINTELLIGENCE MATTERS TO BE REPORTED
TO THE SECURITY MANAGER

5000. BASIC POLICY. Certain matters affecting national security must be reported to the Security Manager, who will report the matter to the NCIS. All military and civilian personnel of this headquarters, whether they have access to classified information or not, will report to the Security Manager, or if on leave/TAD, the nearest command, any activities described in this Chapter involving themselves, their dependents, or others.

1. Sabotage, Espionage, or Deliberate Compromise. Individuals becoming aware of possible acts of sabotage, espionage, deliberate compromise or other subversive activities will notify the Security Manager.

2. Contacts with Citizens of Communist Controlled or Hostile Countries.

a. Any form of contact, intentional or otherwise, with any citizen of a communist controlled country or countries currently hostile to the U.S. must be reported to the Security Manager. The term "contact" means any form of encounter, association, or communication with any citizen of a communist controlled or hostile country, including contacts in person, by radio, telephone, letter, or other forms of communication for social, official, private, or any other reason.

b. This policy applies to all Navy and Marine Corps military personnel on active duty or in an active duty status in the Reserve, and to all civilian personnel employed by the DON.

c. The current list of communist controlled countries and those currently hostile to the U.S. is available from the Security Manager.

3. Suicide or Attempted Suicide. When a member of this headquarters commits suicide or attempts suicide.

4. Unauthorized Absentees. When a member of this headquarters, who has or has had access to classified information is in an unauthorized absence status, the Security Manager must be immediately notified so that a determination can be made to see if there are any indications that the individual's activities, behavior, or associations may be harmful to the interest of national security.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5. Other activities which may cause a persons loyalty to the U.S. to be questioned include the commission of acts of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereat or preparation therefore or conspiring with or aiding or abetting another to commit or attempt to commit any such acts.
6. Criminal or dishonest conduct.
7. Any mental or emotional disorders.
8. Financial mismanagement resulting in excessive indebtedness, recurring financial difficulties or unexplained affluence.
9. Alcohol abuse resulting from habitual or episodic use of intoxicants to excess. This includes arrests for driving while intoxicated (DWI), driving under the influence (DUI), and other alcohol related incidents.
10. Drug abuse, including illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis, or other dangerous drugs.
11. Falsification or the knowing and willful falsification, cover-up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the DoD or any Federal agency.
12. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgement, or lack of regard for the laws of society.

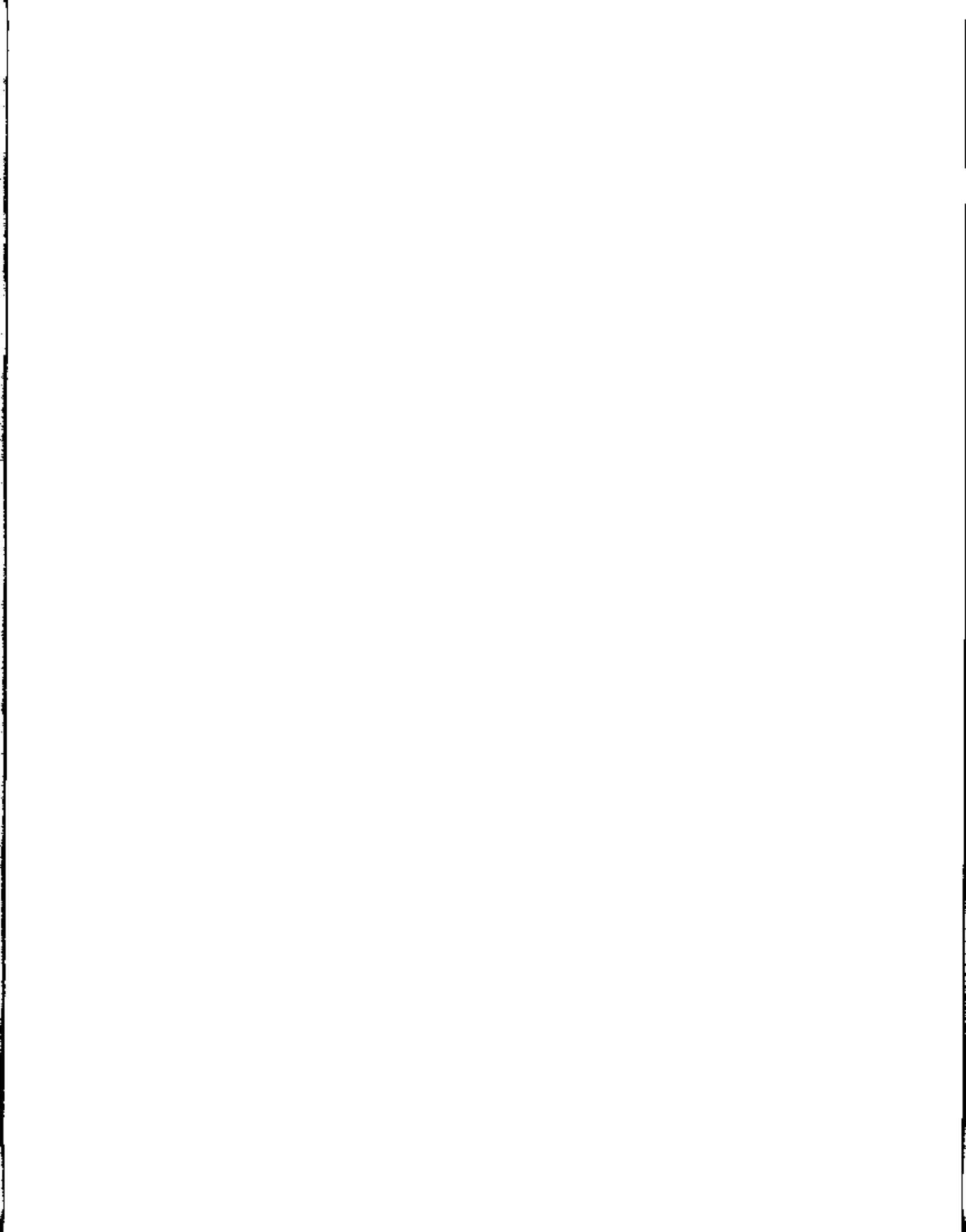
5001. REPORTING RESPONSIBILITIES. The Battalion Commander, the Company Commander, division/branch/section heads and officers in charge who become aware of adverse or derogatory information (including the categories identified above) relative to an individual's personnel security, must notify the Security Manager of the circumstances, to include:

1. The nature of the adverse or derogatory information.
2. An evaluation of the individual's conduct and performance of duty.
3. A recommendation as to whether the individual's security clearance should be terminated for cause.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 6
CLASSIFICATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	6000	6-3
CLASSIFICATION DESIGNATIONS	6001	6-3
ORIGINAL CLASSIFICATION AUTHORITY	6002	6-3
ORIGINAL VERSUS DERIVATIVE CLASSIFICATION.	6003	6-4
ORIGINAL CLASSIFICATION PRINCIPLES AND CONSIDERATIONS.	6004	6-5
SPECIFIC CLASSIFYING CRITERIA	6005	6-7
LIMITATIONS ON CLASSIFYING.	6006	6-7
DURATION OF ORIGINAL CLASSIFICATION	6007	6-8
CHALLENGES.	6008	6-8
TENTATIVE CLASSIFICATION.	6009	6-8
FOREIGN GOVERNMENT INFORMATION.	6010	6-9



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 6

CLASSIFICATION

6000. BASIC POLICY

1. Executive Order 12356 is the only basis for classifying information except as provided in the Atomic Energy Act of 1954, as amended. It is the policy of the DON to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information will be classified only to protect national security.
2. Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, safeguard it as if it were classified at least "Confidential" pending a determination by an original classification authority (OCA). When there is reasonable doubt about the appropriate level of classification, safeguard the information as if it were classified at the higher level until an OCA makes a determination.

6001. CLASSIFICATION DESIGNATIONS

1. Information which requires protection against unauthorized disclosure in the interest of National security must be classified in one of three designations: "Top Secret", "Secret", or "Confidential." The markings "For Official Use Only" and "Limited Official Use" cannot be used to identify classified information, nor can an individual use modifying terms in conjunction with authorized classification designations such as "Secret Sensitive."
2. "Top Secret" is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security.
3. "Secret" is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.
4. "Confidential" is the designation applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

6002. ORIGINAL CLASSIFICATION AUTHORITY

1. The authority to originally classify information as Top Secret,

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

Secret, or Confidential rests with the Secretary of the Navy and designees.

2. Within this headquarters, the COMMARFORPAC is the only individual who has been granted "Top Secret" OCA.
3. When sections within MARFORPAC generate classified material, they will ensure that the material is signed off in the name of the commander. OCA can not be delegated. No other officials within this headquarters have been granted OCA.

6003. ORIGINAL VERSUS DERIVATIVE CLASSIFICATION

1. Original classification is the initial determination that information requires, in the interest of National security, protection against unauthorized disclosure and a determination of the level of protection required.
2. Derivative classification can be accomplished by anyone who incorporates, paraphrases, restates, or generates in new form, information which is already classified. Derivative classification is most commonly accomplished by marking material per the guidance from an OCA.
3. A derivative classifier must:
 - a. Respect original classification decisions.
 - b. Verify the current level of classification of information insofar as it is practicable.
 - c. Carry forward to any newly created documents previously assigned dates or events for declassification, or a notation that the information cannot be automatically declassified without the approval of the originating agency.
4. Information extracted from a classified source will retain the classification markings exactly as shown on the source material. Normally, the overall and internal markings of the source material will provide adequate classification guidance. If the source material lacks internal markings and classification guidance is not included or referenced, classify the extracted material according to the overall marking of the source.
5. Any questions regarding original or derivative classification should be referred to the OIC CMCC or the Security Manager for resolution.

6. Each classifier is accountable for the propriety of the classifications they assign, whether original or derivative. Officials with "By direction" signature authority must ensure that classification markings are accurate before they sign classified material.

6004. ORIGINAL CLASSIFICATION PRINCIPLES AND CONSIDERATIONS.

Since several sections within this headquarters generate classified material that requires OCA, the following should be used as a guide in determining whether information/material should be classified:

1. Evaluate the information to form the basis for classification. Material is classified either because of the information it contains or because of the information it may reveal when associated with other information, including that already officially released into the public domain.

2. Identify the specific elements of information which serve as the basis for a particular national advantage and could, if compromised, adversely affect National security.

3. Weigh the advantages and disadvantages of classifying. The decision to classify must be the result of a reasoned judgement.

4. In arriving at a reasoned judgement, consider the following factors:

a. The degree of intended or anticipated dissemination or use of the information. This factor does not necessarily preclude classification; however, classification may be impractical if wide use or dissemination is expected, such as is involved in medical records or personnel files or maintenance manuals. Similarly, intended use of material in circumstances which preclude realistic protection, such as an aircraft's external appearance, prevents effective classification.

b. Net National Advantage. In exceptional circumstances, other U.S. Government agencies or commercial interests may benefit from the unrestricted use of certain scientific or technical information which is classified or classifiable. Weigh these benefits against the advantage of classifying or continuing classification of the information. This factor should prevail only when an OCA can determine beyond a reasonable doubt that the unclassified use of the information will result in a net advantage to the U.S.

c. Lead Time Advantage (the interval between the time the U.S. Government acquires knowledge and the time we believe other

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

governments can acquire the same knowledge). Obtaining and maintaining a technological and operational lead time is essential to national security. Consider classifying if a lead time advantage would be lost by public release.

d. Consider the cost of classification in terms of time, money, personnel and whether the cost of protecting the information might impede or prevent attainment of the program objective.

e. State of the Art and Intelligence. The state of the art in other nations may be a vital consideration. Evaluate information from intelligence sources to determine the extent to which the information being considered for classification is known or may be available to others. Consider whether it is publicly known that the U.S. possesses the information or is interested in the subject.

f. Effect of Open Publication. Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification. Unofficial publication or inadvertent or unauthorized disclosure does not constitute automatic declassification. Determine the degree of damage which could result by an official declassification and reevaluate the information to decide whether continued protection is required. Holders are required to continue classification until advised otherwise.

g. Scientific Research. Ordinarily, basic scientific research and its results may not be classified (except information which meets the definition of Restricted Data). Classification is appropriate, however, if the information concerns an unusually significant scientific "breakthrough", is beyond the state of the art of other nations, and supplies the U.S. with an advantage directly related to the national security.

h. Compilation of Information. Normally, a compilation of unclassified items of information may not be classified. Certain information that would otherwise be unclassified may, however, require classification when combined or associated with other unclassified information. In unusual circumstances, the combination of unclassified items of information may provide an added factor and warrant classification. Fully support, in writing, any classification on this basis and provide the explanation on or with the material. The Security Manager or AC/S G-3 OPSEC Officer can provide assistance in making classification decisions with regard to a compilation of information.

6005. SPECIFIC CLASSIFYING CRITERIA

1. There are two decisions to be made by an OCA in making a determination to classify in the original classification process: First, that the information meets one or more of the criteria in subparagraphs 2a through 2j; and second, that unauthorized disclosure of the information could cause damage to National security. Because information may fall under one or more of the criteria below, do not presume that it automatically meets the damage criterion.

2. Consider classifying information if it concerns:

- a. Military plans, weapons, or operations.
- b. Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security.
- c. Foreign government information.
- d. Intelligence activities (including special activities), or intelligence sources or methods.
- e. Foreign relations or foreign activities of the U.S.
- f. Scientific, technological, or economic matters relating to national security.
- g. U.S. Government programs for safeguarding nuclear materials or facilities.
- h. Cryptology.
- i. A confidential source.
- j. Other categories of information related to national security and requiring protection against unauthorized disclosure as determined by the Secretary of the Navy.

3. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source or intelligence sources or methods, is presumed to cause damage to the national security. The level of classification is dependent on the anticipated degree of damage.

6006. LIMITATIONS ON CLASSIFYING

1. Original classifiers within this headquarters may not:

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

- a. Use classification to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.
- b. Classify basic scientific research information which is not clearly related to National security.
- c. Classify a product of non-Governmental research and development, that does not incorporate or reveal classified information to which the producer or developer was given prior access, unless the Government acquires a proprietary interest in the product.
- d. Classify, or use as a basis for classification, references to classified documents when the reference citation does not in itself disclose classified information.
- e. Use classification to limit dissemination of information that is not classifiable under this Manual or to prevent or delay the public release of the information.

6007. DURATION OF ORIGINAL CLASSIFICATION

1. Information will be classified for as long as required by National security considerations. Assign dates or events for declassification whenever possible.
2. If a date or event for declassification cannot be predetermined, provide for an indefinite duration of classification. (See chapter 9 of this Manual.)
3. Only OCAs may extend a specified duration of classification and only if all known holders of the information can be notified prior to the date or event originally set for declassification.

6008. CHALLENGES. If there is substantial reason to believe that information is classified improperly or unnecessarily, the matter will be referred to the Security Manager for review.

6009. TENTATIVE CLASSIFICATION. All staff sections that originate information believed to contain classified information, will take the following precautions:

1. Safeguard the information for intended classification.
2. Mark the information with the intended classification, preceded by the word "tentative."

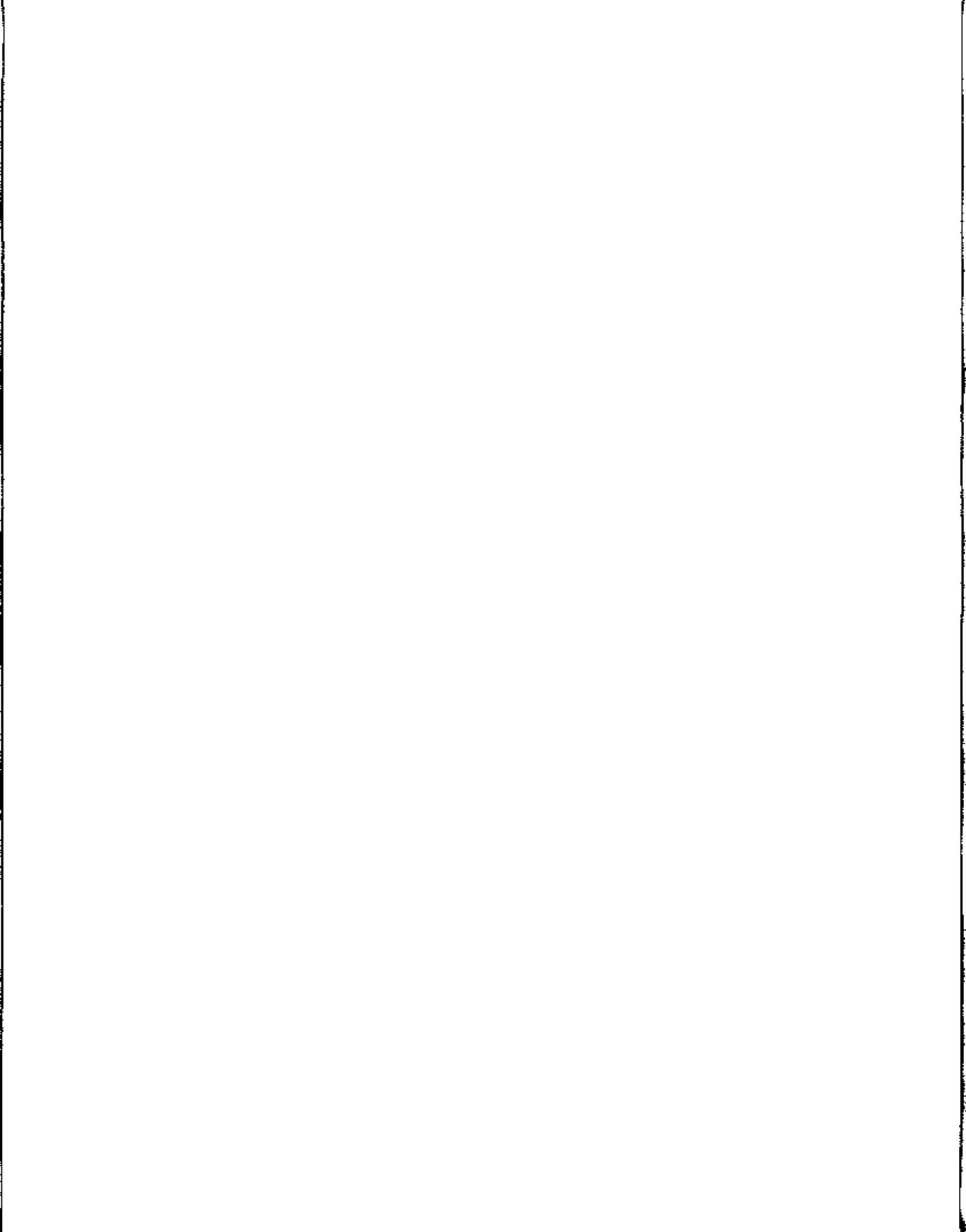
3. Forward the information to an official identified in paragraph 6002 above for a security determination. If a determination cannot be made, then the material will be forwarded to the Security Manager for review.

6010. FOREIGN GOVERNMENT INFORMATION. Occasionally, this headquarters receives classified information originated by a foreign government. The following guidelines pertain to the protection of foreign government information.

1. Information classified by a foreign government or international organization retains its original classification designation, or is assigned a U.S. designation that will provide protection equivalent to that provided by the originator of the information. Authority to assign the U.S. designation does not require an OCA.

2. Foreign government information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence, must be classified by an OCA. Because Executive Order 12356 presumes damage to the national security will occur if that information is disclosed, foreign government information must be classified at least Confidential. It may be classified at a higher level if it meets the damage criteria of paragraph 6001 above.

3. Do not assign a date or event for automatic declassification to foreign government information unless specified or agreed to by the foreign entity. Foreign government information classified by the DON, will be protected for an indefinite period and will be marked to be declassified upon original authority declassification required (OADR).

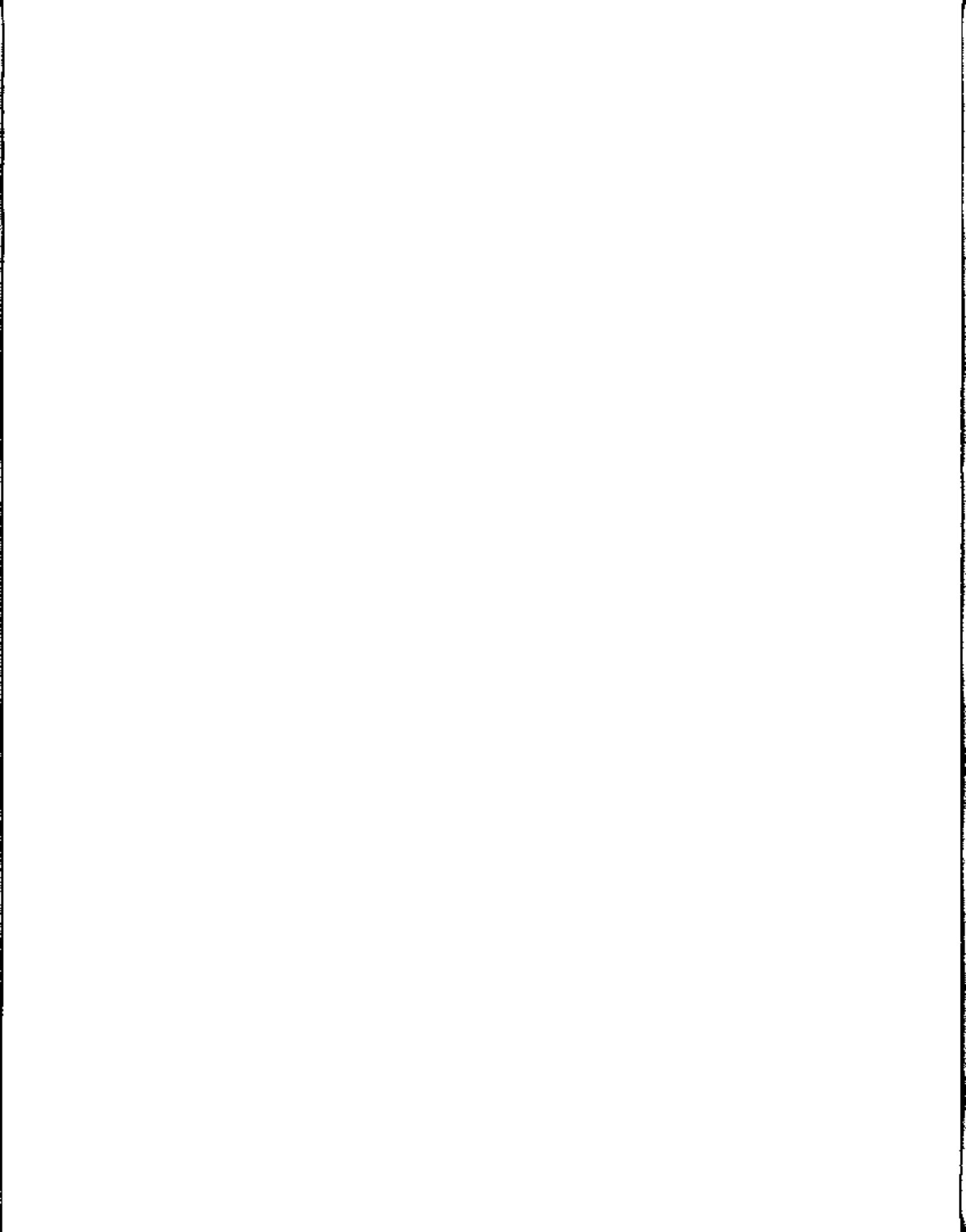


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 7

CLASSIFICATION GUIDES

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	7000	7-3
RETRIEVAL AND ANALYSIS OF NAVY CLASSIFIED INFORMATION (RANKIN)	7001	7-3
ORIGINATING SECURITY CLASSIFICATION GUIDES.	7002	7-4



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 7

CLASSIFICATION GUIDES

7000. BASIC POLICY. Security classification guides in the current editions of OPNAVINST 5513 series, are produced to help in the identification and proper classification of various Navy and Marine Corps programs. Classification guides are excellent "tools" to use in making security classification determinations and should be consulted on a routine basis.

7001. RETRIEVAL AND ANALYSIS OF NAVY CLASSIFIED INFORMATION (RANKIN)

1. RANKIN is a computerized program providing standardization, centralized management, and promulgation of all DON security classification guides. It provides a central storage and retrieval system for classification guidance.

2. Uniformly formatted classification guides are issued in the following major subject categories:

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

b. OPNAVINST C5513.2: Air Warfare Programs (U).

c. OPNAVINST S5513.3: Surface Warfare Programs (U).

d. OPNAVINST S5513.4: General Intelligence, Cover and Deception, and Investigative Programs (U).

e. OPNAVINST S5513.5: Undersea Warfare Programs (U).

f. OPNAVINST S5513.6: Communication and Satellite Programs (U).

g. OPNAVINST C5513.7: Mine Warfare Programs (U).

h. OPNAVINST S5513.8: Electronic Warfare Programs (U).

i. OPNAVINST S5513.9: Nuclear Warfare Programs (U).

j. OPNAVINST C5513.10: Miscellaneous Programs (U).

k. OPNAVINST 5513.11: Ground Combat Systems (U).

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

1. OPNAVINST S5513.12: Intelligence Research Projects (U).
 - m. OPNAVINST S5513.13: Non-Acoustic Anti-Submarine Warfare (U).
3. The OPNAV instruction for each major subject area contains, as enclosures, individual classification guides for programs, projects, plans, or systems related to the overall subject area of the instruction. Most staff sections retain classification guides for information under their cognizance. The Security Manager maintains a complete volume of the above listed classification guides.

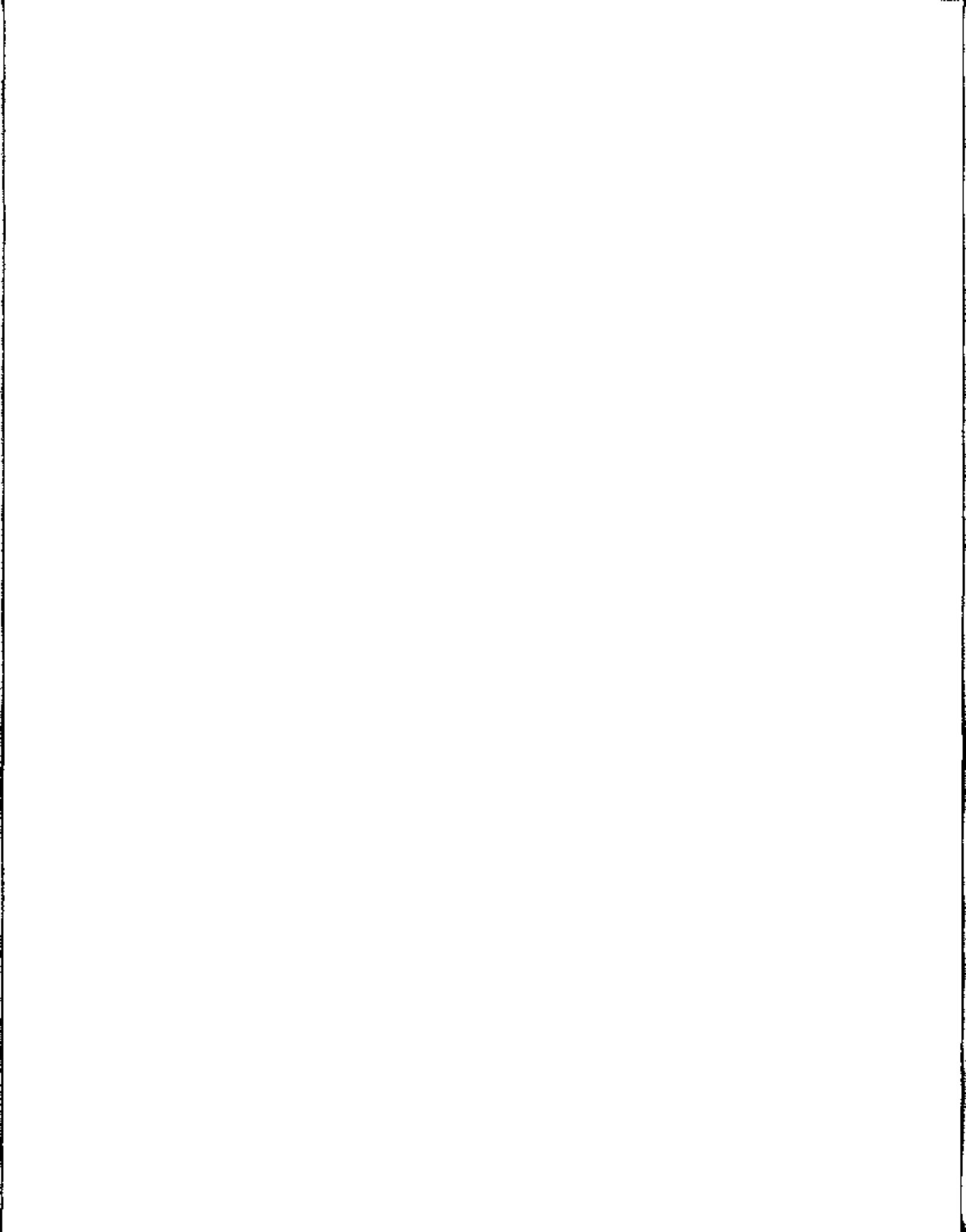
7002. ORIGINATING SECURITY CLASSIFICATION GUIDES. Divisions and separate branch heads will not originate classification guides without the approval and guidance of the Security Manager.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	8000	8-3
DECLASSIFICATION AND DOWNGRADING AUTHORITY	8001	8-3
SYSTEMATIC DECLASSIFICATION REVIEW.	8002	8-3
UPGRADING	8003	8-4
NOTIFICATION.	8004	8-4



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 8

DECLASSIFICATION, DOWNGRADING AND UPGRADING

8000. BASIC POLICY. Information classified by MARFORPAC will be declassified as soon as national security considerations permit. Decisions concerning declassification or downgrading must be based on the loss of sensitivity of the information with the passage of time or the occurrence of an event which permits declassification or downgrading. Information that continues to meet the classification criteria of paragraph 6002 of this Manual, despite the passage of time, must be protected.

8001. DECLASSIFICATION AND DOWNGRADING AUTHORITY

1. Within this headquarters, the following officials are authorized to declassify and downgrade classified information originated within this command:

a. Commander.

b. Other individuals granted original classification authority identified in paragraph 6002 of this Manual, a successor or supervisor or either.

2. The officials designated are the only ones who may decide that specific information no longer requires the protection originally assigned, that is, change the original classification determination with a resulting change in the classification guidance for that information. The authority to downgrade or declassify is not to be confused with the administrative responsibility of a holder of classified information to downgrade or declassify it as directed by a classification guide, the continued protection guidelines, or the instructions on a document. Note that this paragraph speaks only to the authority to downgrade or declassify. See paragraph 6007 of this Manual for authority to extend the duration of classification and paragraph 8003 following for authority to upgrade the classification.

8002. SYSTEMATIC DECLASSIFICATION REVIEW. This headquarters is no longer required to conduct a systematic review for declassification. In the interest of reducing classified holdings, all divisions and separate branches will continuously evaluate the need to maintain classified documents with the goal of keeping these holdings to a minimum. Classified information relating to MARFORPAC that is required to be maintained for historical purposes, should be returned to CMCC for retention. Classified

documents will not be maintained for the sole purpose of plagiarizing at some unknown time.

8003. UPGRADING

1. Original classification authorities identified in paragraph 6002 of this Manual, may upgrade classified information within their functional areas of interest only when:

a. All known holders of the information can be promptly notified.

b. All known holders of the information are authorized access to the higher level of classification.

c. The information can be retrieved from the known holders not authorized access to the higher level of classification.

2. Information previously determined to be unclassified may be classified only when the OCA determines that the provisions of paragraph 8003.1 above have been met, that control of the information has not been lost, and that loss of control can still be prevented.

8004. NOTIFICATION. Notices are not issued to downgrade or declassify material marked with specific events for downgrading or declassification. If classified information, originally classified within this headquarters, is extended or decreased as a result of an unscheduled change to shorten or lengthen duration, or if change to the classification level is made, all original addressees will be notified of the change. A notice assigning classification to currently unclassified information will be classified Confidential, unless the notice itself contains information at a higher level.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 9

MARKING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	9000	9-3
BASIC MARKING REQUIREMENTS.	9001	9-3
OVERALL AND PAGE MARKINGS ON PUBLICATIONS . .	9002	9-4
OVERALL AND PAGE MARKING ON CORRESPONDENCE. .	9003	9-5
PORTION MARKINGS.	9004	9-6
COMPILATIONS.	9005	9-6
SUBJECTS AND TITLES	9006	9-6
FILES, FOLDERS, OR GROUPS OF DOCUMENTS. . . .	9007	9-7
TRANSMITTALS.	9008	9-7
ELECTRONICALLY TRANSMITTED MESSAGES	9009	9-7
CHARTS, MAPS AND DRAWINGS	9010	9-7
PHOTOGRAPHS	9011	9-8
TRANSPARENCIES AND SLIDES	9012	9-8
RECORDINGS.	9013	9-8
DECKS OF AUTOMATIC DATA PROCESSING PUNCHED CARDS	9014	9-8
REMOVABLE AUTOMATIC DATA PROCESSING AND WORD PROCESSING STORAGE MEDIA	9015	9-9
DOCUMENTS PRODUCED BY ADP EQUIPMENT	9016	9-9
FOREIGN GOVERNMENT INFORMATION.	9017	9-9
MISCELLANEOUS MATERIAL.	9018	9-10
DOWNGRADING, DECLASSIFICATION OR UPGRADING	9019	9-10

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

REMARKING OLD MATERIAL.	9020	9-11
STANDARD DOWNGRADING/DECLASSIFICATION MARKINGS.	9021	9-11
MATERIAL WITHOUT DECLASSIFICATION MARKINGS.	9022	9-12
WARNING NOTICES	9023	9-12
SECURITY DISCREPANCY NOTICE	9024	9-12

FIGURE

9-1 MARKINGS FOR THE COVER OF A DOCUMENT	9-13
9-2 MARKINGS FOR INTERIOR PAGES OF A DOCUMENT.	9-14
9-3 CLASSIFIED MARKINGS FOR A NAVAL LETTER	9-16
9-4 PORTION AND PARAGRAPH MARKINGS	9-17
9-5 MARKINGS FOR A MEMORANDUM.	9-18
9-6 MARKINGS FOR ILLUSTRATIONS	9-19
9-7 MARKINGS FOR A LETTER OF TRANSMITTAL	9-20
9-8 MARKINGS FOR A MESSAGE	9-21
9-9 MARKING GUIDE FOR PUBLICATIONS AND CORRESPONDENCE. . .	9-22

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 9

MARKING

9000. BASIC POLICY

1. Classified material will be physically marked, annotated, or identified by other means, as prescribed in this chapter. 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 declassifying actions. Therefore, all classified material must be marked in a manner that leaves no doubt about 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.

2. Classified material is any product embodying classified information. Where the word "document" is used in this Manual, it means publications (bound or unbound, printed material such as reports, studies, manuals), correspondence (such as military and business letters and memoranda), and other printed or written products (such as charts, maps). Most documents are easily marked, while other material such as hardware, recordings, photographs, etc., may be more difficult to identify because of physical characteristics.

9001. BASIC MARKING REQUIREMENTS

1. Marking requirements and the application of markings vary, depending on the kind of material. Basic markings required for all classified material are:

a. For originally classified material:

- (1) The identity of the original classification authority.
- (2) The agency or office of origin.
- (3) The overall classification.
- (4) The declassification date or event or the notation,

OADR.

- (5) Any downgrading instructions.

b. For derivatively classified material:

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

(1) The source of classification (e.g., source document or classification guide), including its date when necessary for positive identification. If you derive classification from more than one source, use the phrase, "Multiple Sources." Drafters will keep a listing of the multiple sources with the command file or record copy of a document or the related or accompanying documentation for other kinds of classified material. (The listing is not distributed with the material.)

(2) The agency and office of origin.

(3) The overall classification.

(4) The declassification date or event, or the notation, OADR. If you derive classification from multiple sources, carry forward the most remote date or event for the declassification marked on any of the sources. OADR is the most restrictive declassification instruction. If any source has this notation, you must use it instead of a declassification date.

(5) Any downgrading action required.

2. In addition to the foregoing, some material may require warning notices and/or intelligence control markings as described in paragraph 9023 following. Derivatively classified material will carry any warning notices or control markings from its sources that also apply to the new material.

3. Stamp, print, or write classification markings in capital letters larger than those used in the text of a document or conspicuously on other material, and, when practicable, colored red.

4. Figures 9-1 through 9-8 are appended to this chapter with illustrations of markings. Figure 9-9 is a detailed marking guide for publications and correspondence. The text of the figures also provides amplification of marking requirements and should be read for additional guidance.

9002. OVERALL AND PAGE MARKINGS ON PUBLICATIONS

1. Place the basic markings on the face of the publication, that is the front cover or title page or first page, whichever is the front of the publication. Place the overall classification at the top and bottom center of the front cover (if any), the title page, (if any) and the first page. Downgrading and declassification instructions appear only on the face of the publication.

2. A back cover is not required. If used, place the overall

classification at the top and bottom center. Associated markings are not placed on the back cover. If a back cover is not used, classified text may not appear on the back of the last page and the overall classification will be placed at the top and bottom center of the back page. Examples of cover page markings are in figure 9-1.

3. Mark the classification of each interior page of a publication at the top and bottom center of the page. Normally, the overall classification of the publication is used. This procedure is recommended because it is simpler, more efficient, and satisfies the security objective. Originators do have the option, however, of marking each interior page with the highest classification it contains. If an originator exercises this option and the page is printed on front and back, both sides of the page must be marked with the highest classification of either side. When one of the sides contains information of a lower classification than the marking applied, include a statement such as "This page is Unclassified", or "This page is Confidential."

4. Do not put downgrading/declassification instructions on interior pages and do not spell out warning notices on interior pages. The originator is required to place the short form of the intelligence control markings that apply to that page either at the top or bottom of the page, after the classification marking (e.g., SECRET/WNINTEL). Examples of interior page markings are in figure 9-2.

9003. OVERALL AND PAGE MARKINGS ON CORRESPONDENCE

1. Place the basic markings on the first page of correspondence. Type the overall classification on the first page at the upper left and stamp it at top and bottom center. Place the classification authority, downgrading and declassification instructions at the lower left. Spell out warning notices after the typed classification at the upper left except those for Restricted Data or Formerly Restricted Data.

2. On second and succeeding pages, stamp the classification on the top and bottom center. The classification may be the overall classification or the highest classification of information on that page. Place the short form of any intelligence control marking that applies to information on a page after the classification either at the top or bottom of the page (e.g., SECRET/WNINTEL). Examples of correspondence markings are in figures 9-3, 9-4 and 9-5.

9004. PORTION MARKINGS

1. Mark each portion (section, part, paragraph, or subparagraph) of a classified document, to show the level of classification or the fact that it is unclassified. The intention of this requirement is to eliminate any doubt as to which portions of a document contain or reveal information requiring protection. It is essential, however, to consider each portion or classification on the basis of its content and its association with other information. Place the appropriate symbol immediately following the portion letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. The parenthetical symbols are: (TS) for Top Secret, (S) for Secret, (C) for Confidential, (FOUO) For Official Use Only, and (U) for Unclassified. Add to the classification symbols, as appropriate, the abbreviated form for Restricted Data, Formerly Restricted Data, or Critical Nuclear Weapons Design Information, e.g., (S-RD), (C-FRD), or (S-RD)(N). Portion mark also with the abbreviated form of the intelligence control marking, e.g., (S-NF) or (S-WN), etc. Examples of portion marking are in figures 9-3 and 9-4.

2. Mark the classification in full, not the abbreviated form, on figures, tables, graphs, charts, photographs, and similar illustrations incorporated in classified documents.

9005. COMPILATIONS. When classification is required to protect a compilation of information (see paragraph 6004 of this Manual), place an additional statement on the face of the document explaining the reasons for the classification. The statement must include:

1. The fact that the individual parts are of a lower classification.
2. The reason why the compilation warrants a higher classification.
3. The authority for the classification.

9006. SUBJECTS AND TITLES. Whenever possible, subjects or titles of documents will be unclassified to simplify referencing them in unclassified documents or indexes. If a classified subject is necessary to convey meaning, add an unclassified short title for reference purposes. Mark subjects or titles with the appropriate parenthetical symbol (TS), (S), (c), (FOUO), or (U) immediately following the subject. When subjects or titles of classified documents are included in the reference line, enclosure line, or

body of a document, the classification of the subject or title follows. (See figure 9-3.)

9007. FILES, FOLDERS OR GROUPS OF DOCUMENTS. When a file, folder or group of classified documents are removed from secure storage, mark them conspicuously with the highest classification of any classified document they contain, or attach an appropriate classified document cover sheet.

9008. TRANSMITTALS. When a transmittal document or endorsement 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. For example, an unclassified letter which transmits a classified document as an enclosure, would carry the classification of the enclosure and the notation, "Unclassified upon removal of the enclosure. "Warning Notices", intelligence control markings, or special notations on the enclosures are also shown on the transmittal. Include downgrading and declassification instructions only when the transmittal itself is classified. Otherwise, the notation that the transmittal is unclassified when the enclosure is removed is the only instruction needed. Figure 9-7 is a sample letter of a transmittal.

9009. ELECTRICALLY TRANSMITTED MESSAGES

1. Mark classified messages at the top and bottom with the overall classification and portion mark as prescribed for other documents.
2. The last line of text of a classified, electrically transmitted message must show the date or event for declassification or the notation "Originating Agency's Determination Required", using the abbreviated markings illustrated in figure 9-8. Messages containing Restricted Data or Formerly Restricted Data do not require the downgrading or declassification annotation; however, the originator's record copy must indicate the basis of classification.

9010. CHARTS, MAPS AND DRAWINGS. Charts, maps and drawings that are separate classified documents are marked differently from those used as illustrations in classified documents (see figure 9-6). Mark the overall classification at the top and bottom of each document. Place the classification of the legend, title block or scale under the legend, title block or scale in a manner that differentiates it from the classification assigned to the document as a whole. All materials delivered to the Training and Audio-

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

visual Support Unit (TAVSU) will be properly marked by the preparing division/branch prior to the project being initiated. Figure 9-6 identifies the correct marking procedures for illustrations.

9011. PHOTOGRAPHS

1. When practicable, the Force TAVSU will mark photograph negatives and contact sheets with the classification and associated markings and keep them in containers that have conspicuous markings.

2. All prints will be marked with the classification at the top and bottom on the face side, and with the associated markings at the bottom. The classification need only be applied once on smaller prints. Whenever it is not practicable to place classification and associated markings on the face of prints, place the markings on the reverse side, using a pressure tape label or a stapled strip if stamping is not practicable. All reproductions of a photograph must clearly show classification and associated markings such as downgrading and declassification.

9012. TRANSPARENCIES AND SLIDES. Clearly show the classification and associated markings on the border, holder, or frame and whenever possible, on the image of each transparency or slide. When transparencies or slides are reproduced as part of hard copy test material, make sure the markings are included. All viewgraphs will be prepared with the classification printed on the transparency. The preparing division/branch is responsible for properly marking these materials, not the Force TAVSU. Figure 9-6 identifies the correct marking procedures for transparencies and slides.

9013. RECORDINGS. Make a clear statement of the assigned classification at the beginning and end of each sound or electronic recording to ensure that listeners or viewers understand that classified information is involved. Keep recordings in containers or on reels conspicuously marked with the classification and associated markings.

9014. DECKS OF AUTOMATIC DATA PROCESSING PUNCHED CARDS. When a deck of classified automatic data processing punched cards is handled and controlled as a single document, only the first and last cards require classification markings. Add an additional card (or modify the job control card) to identify the contents of the deck, the highest classification and associated markings. Cards

removed for separate processing or use and not immediately returned to the deck will be marked individually.

9015. REMOVABLE AUTOMATIC DATA PROCESSING AND WORD PROCESSING STORAGE MEDIA

1. External Markings. Removable information storage media and devices, used with automatic data processing (ADP) systems and typewriters or word processing systems, must be marked externally to indicate clearly the classification of the information they contain and the associated markings. Media and devices that store information recorded in analog or digital form and are generally mounted or removed by the users or operators, include; magnetic tape reels, cartridges and cassettes, removable disks, disk cartridges, disk packs, and diskettes, paper reels and magnetic cards.

2. Internal Markings. ADP systems and word-processing systems will be programmed to provide for internal markings of paper products to ensure that classified information, which is reproduced or generated, clearly shows the classification and associated markings.

9016. DOCUMENTS PRODUCED BY ADP EQUIPMENT. Mark the first page and the front and back covers, if any, of documents produced by ADP equipment as prescribed in paragraph 9003 above. Classification markings of interior pages may be applied by the ADP equipment or by other means. When it is not economical or efficient for the ADP equipment to apply the associated markings prescribed in paragraph 9002 above, the markings may be applied to a document produced by ADP equipment by superimposing upon the first page a "Notice of Declassification Instructions and Other Associated Markings." This notice must show the date or event for declassification, or the notation "OADR" and all other associated markings.

9017. FOREIGN GOVERNMENT INFORMATION

1. NATO Documents. Classified documents originated by NATO, if not already marked with the appropriate classification in English, will be so marked. Do not place downgrading/declassification markings, required for U.S. originated documents, on documents originated by NATO. On documents originated by NATO that are marked Restricted, make the following additional notation: "To be safeguarded in accordance with USSAN Instruction 1-69." (USSAN Instruction 1-69 was promulgated by OPNAVINST C5510.101).

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

2. Other Foreign Government Documents. Foreign security classifications generally parallel U.S. classifications. If the classification of foreign government documents is shown in English, no additional classification marking is required. Do not apply the downgrading/declassification markings required for U.S. originated documents.

3. NATO or Foreign Government Information in DON Documents. Unless the markings would reveal intelligence information, identify NATO or foreign government information incorporated in DON documents in a manner to ensure that the information is not prematurely declassified nor made accessible to nationals of a third country without the consent of the originator. Mark the face of the document, "FOREIGN GOVERNMENT INFORMATION," or, if the document incorporates or contains extracts of NATO classified information, "This document contains NATO classified information." Documents with the latter marking do not require transmission through NATO channels. Include the appropriate identification in the portion markings, e.g., (NATO-S), (U.K.-C), or (FRG-Restricted). Enter the "Classified by" line and the notation "Originating Agency's Determination Required" on the document even though it may contain only foreign government information.

9018. MISCELLANEOUS MATERIAL. Material such as rejected copies, typewriter ribbons, carbons, and similar items developed in connection with the handling, processing, production, and use 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. There is a need to mark, stamp, or otherwise indicate that the recorded information is classified to ensure its protection. All Top Secret waste will be turned over to the Top Secret Control Officer for destruction.

9019. DOWNGRADING, DECLASSIFICATION OR UPGRADING. Upon notification that information has been upgraded or that the downgrading and declassification instructions have been changed, the holder must promptly and conspicuously mark the material containing the information to indicate the change, the authority for the action, the date of the action, and identity of the person making the change. Cancel all the old markings if practicable. At a minimum, place the new classification marking (including "Unclassified") on the cover (if any) and on the first page. For example, if you are notified by message from HQMC that a Secret HQMC letter you hold has been declassified, remark at least the cover (or if none, the first page) as Unclassified at the top and bottom, and identify the authority: "Declassified by CMC 151634Z November 1982 on 18 November 1982 by I. M. Marine, AC/S G-3."

9020. REMARKING OLD MATERIAL

1. Classified material marked for automatic downgrading or declassification on a specific date or event will be downgraded or declassified accordingly. You need not remark this material. Any information extracted from this material will carry forward any future downgrading/declassification date.
2. Classified material that does not carry a specific date or event for automatic downgrading or declassification or does not have any downgrading/declassification instructions, may not be downgraded or declassified without authorization of the originator.
3. Any questions regarding downgrading or declassification of old material will be referred to the Security Manager or the OIC CMCC prior to declassifying the information.

9021. STANDARD DOWNGRADING/DECLASSIFICATION MARKINGS

1. Mark all classified material with the following standard marking:
 - a. Classified by (See Note 1).
 - b. Declassify on (See Note 2).
 - c. Downgrade to (See Note 3).
2. Mark U.S. documents containing foreign government information as follows:
 - a. Classified by (See Note 4).
 - b. Declassify on (See Note 5).

NOTE 1. If original classification, insert identification of the original classification authority (i.e., AC/S G-5). If derivative classification, insert identity of the security classification guide, source document, or other authority for classification. If more than one source is applicable, insert the words "Multiple Sources."

NOTE 2. Insert the specific date or event certain to occur. If a specific date or event cannot be determined, then use the notation, "Originating Agency's Determination Required", or "OADR." When classification is derived from multiple sources, use the declassification date of longest duration applicable to any of the source material in the new material. If a specific

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

date or event cannot be determined or a source document is marked as Review for Declassification, insert the notation "Originating Agency's Determination Required" or "OADR."

NOTE 3. Use this marking only when downgrading is applicable. Insert "Secret" or Confidential" and specific date or event, e.g., "Downgrade to Confidential on 6 July 1984." For messages, abbreviate "S" or "C" to indicate the downgrading classification and give the specific date or event, e.g., "DG/C/6 JUN 83."

NOTE 4. Insert the identity of the foreign source document, memorandum of understanding, or classification guide.

NOTE 5. Insert the notation "Originating Agency's Determination required" or "OADR."

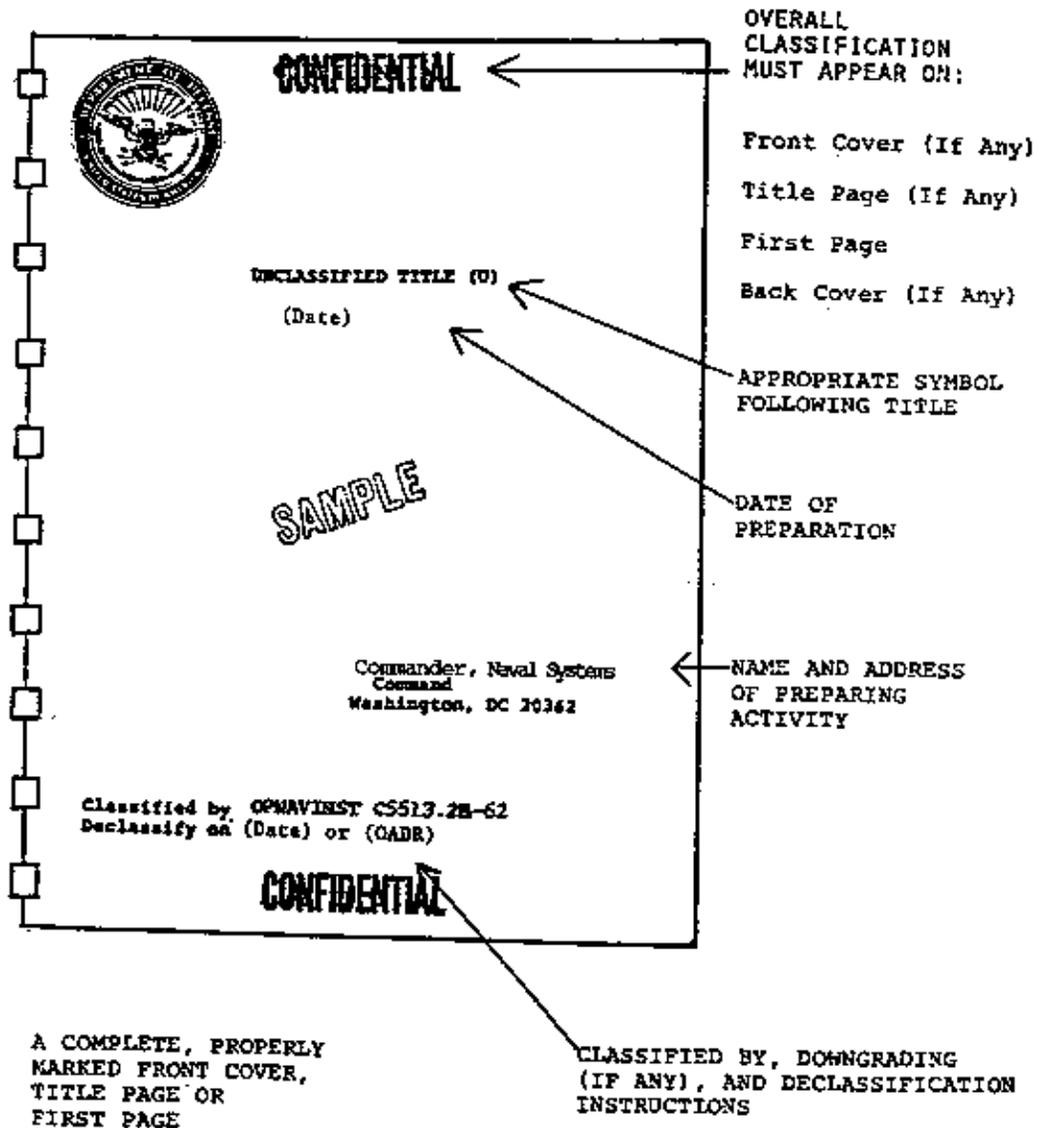
9022. MATERIAL WITHOUT DECLASSIFICATION MARKINGS. If classified material, prepared after 1 August 1982, does not contain declassification instructions, refer it to the Security Manager or the OIC CMCC for appropriate action.

9023. WARNING NOTICES

1. Warning notices advise holders of some special status of information which requires additional protective measures such as restrictions on reproduction, dissemination, or extraction. Placement of warning notices is shown in figure 9-9.
2. A listing of approved warning notices and intelligence control markings is contained in the current edition of OPNAVINST 5510.1.

9024. SECURITY DISCREPANCY NOTICE. When classified material is received in this headquarters which is improperly or incompletely marked, or which does not show proper downgrading or declassification information, notify the OIC CMCC or the Security Manager so that the originator will be advised.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM



NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-1.--Markings for the Cover of a Document.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SECRET

CHAPTER 5

FIRST ORDER HEADING (U)

Second Order Heading (U)

SAMPLE

A. (U) Summary

1. (S) The classification marking of headings is illustrated above. Headings are marked according to their own classification and do not reflect the overall classification of the material which follows. Once a heading is identified by some means, it becomes a paragraph for marking purposes, e.g., "A. (U) Summary", as shown.

2. (U) The classification marking of paragraphs and subparagraphs is the same as for naval letter format. The classification of the lead-in portion of a paragraph is shown at the beginning of the paragraph even though a subparagraph may reveal a higher or lower level of classification

a. (C) Subdivisions need not be marked if they do not express a complete thought. As an example, the following do not express complete thoughts:

- (1) Systematized digital projection
- (2) Compatible organizational flexibility
- (3) Synchronized transitional contingency

b. (U) Individual paragraphs are classified according to the information they reveal.

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-2.--Markings for Interior Pages of a Document.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SECRET

c. (S-NF) Intelligence control markings are shown on the front cover (if any), title page (or first page) and other applicable pages of a document. Interior pages will be marked with the short form of the control marking, that is NOFORN for Not Releasable to Foreign Nationals; WNINTEL for Warning Notice- Intelligence Sources or Methods Involved. Tables, figures and charts will be marked in a similar manner as illustrated in exhibit 9E. Paragraphs and subparagraphs will be marked with the abbreviated form such as NF for Not Releasable to Foreign Nationals; WN for Warning Notice - Intelligence Sources or Methods Involved, etc.

3. (U) The classification markings (top and bottom) should be bold and immediately distinguishable from the text.

2

SECRET/NOFORN

NOTE: SECRET FOR TRAINING OTHERWISE UNCLASSIFIED

Figure 9-2.--Markings for Interior Pages of a Document..Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM



SECRET
DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20380

IN REPLY REFER TO

5510
Ser XXX/S123456
(Date)

SECRET

From: Chief of Naval Operations
To: Recipients

Subj: PORTION MARKING (U)

1. (U) This is a sample of a fairly complex letter with multiple parts (paragraphs, subparagraphs, and a chart). It has been created for the purpose of demonstrating the proper method of applying portion classification markings in accordance with the requirements of OPNAVINST 5510.3. In this sample, paragraph 1 in its totality contains Secret information, but the lines of the opening paragraph do not, as indicated by "U" precursory marking.

a. (S) In continuing the graphic illustration of the proper techniques of applying portion classification markings, this subparagraph of the sample document contains information classified Secret as indicated by the "S" precursory marking.

(1) (S) Again, this subparagraph contains information classified Secret.

(a) (C) Every part of a classified document is to have portion classification markings applied. The text in this subparagraph contains information classified Confidential.

1. (S) The text in this subparagraph contains information that is Secret. Bear in mind that the objective of portion classification marking is to eliminate doubt as to which portions of a document contain or reveal classified information.

a. (U) This part of the sample document is unclassified as indicated by the "U" precursory marking.

b. (C) This part of the sample document is classified Confidential as indicated by the "C" precursory marking.

2. (U) This part contains no classified information.

Classified by OPNAVINST 5510.3A-17
Declassify on OADR

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-3.--Classified Markings for a Naval Letter.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SECRET

Subj: PORTION MARKING (U)

(b) (C) The text in this subparagraph contains information that is classified Confidential.

(2) (U) The text in this subparagraph contains no classified information as shown by the "U" precursory marking. However, the information revealed by the chart that follows is classified Confidential.

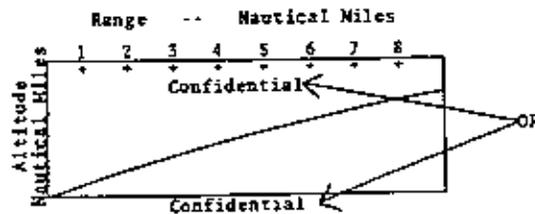


Chart No. 1 (U) Test Results

b. (U) If the above chart were to occupy an entire page, in a briefing book for example, it would still be necessary to mark separately the classification of the chart and its caption. The classification marking of the chart is so placed as not to be confused with the page markings. The text in this subparagraph is unclassified.

2. (U) It should be noted that this letter has been page marked according to its overall classification.

R. R. CORENA
By direction

2

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-4.--Portion and Paragraph Markings.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM



CONFIDENTIAL
DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20338

5510 IN REPLY REFER TO
Ser XXX/C123456
(Date)

CONFIDENTIAL

MEMORANDUM FOR RECIPIENTS

Subj: PORTION MARKING SPECIAL FORMATS (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 those 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

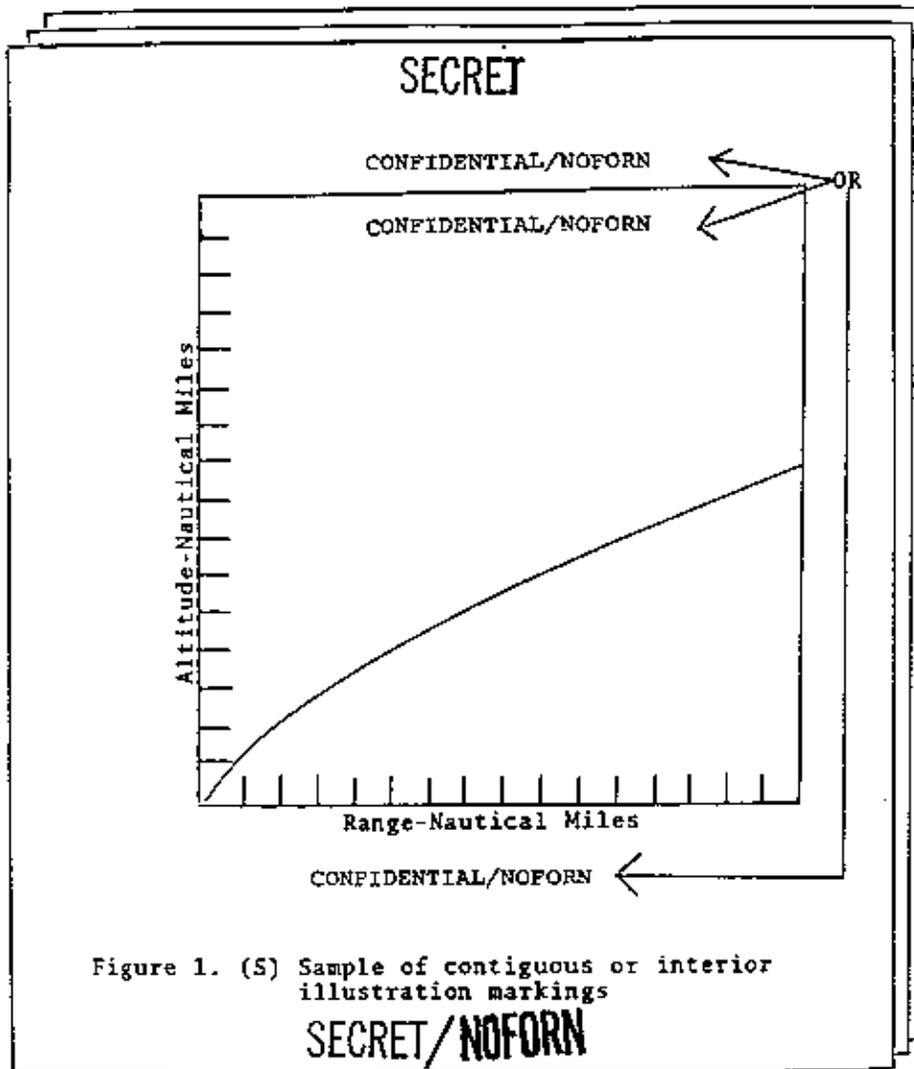
Classified by OPNAVINST 5513.5A-16
Declassify on OADR

CONFIDENTIAL

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-5.--Markings for a Memorandum.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM



Illustrations, figures, tables, graphs, drawings, charts and similar portions of classified documents must be clearly marked to show their classification. Place the marking close to, or within the illustration, etc., as shown above. Captions will be marked, on the basis of their own content, with the symbol (TS), (S), (C) and (U) immediately preceding the caption.

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-6.--Markings for Illustrations.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM



CONFIDENTIAL
DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20380

5510 IN APPLICABLE CASES
Ser XXX/C123456
(Date)

CONFIDENTIAL--Unclassified 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 0123452 Feb 82

Encl: (1) NAVSEA Report 1410, The New Torpedo (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. CORENA
By direction

CONFIDENTIAL

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

Figure 9-7.--Markings for a Letter of Transmittal.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

MARKING GUIDE FOR PUBLICATIONS AND CORRESPONDENCE

(Refer to OPNAVINST 5510.1 for marking requirements for other types of material)

*Required Marking.

MARKING	PLACEMENT
* Classification - TOP SECRET, SECRET OR CONFIDENTIAL.	<p>On publications, stamped or printed TOP and BOTTOM center in letters larger than other print, preferably in red, on the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). If the back cover is not used, classified text may not appear on the back of the last page. Mark interior pages of publications either with the overall classification or with the classification of the individual page. When exercising the individual page option in cases of front and back printing, both sides of the page must be marked with the highest classification of either side. The side with the lower classification should be indicated at the bottom with the statement "This page is Unclassified" or other classification as appropriate.</p> <p>On the first page of correspondence, typed at the upper left in addition to the markings described above.</p>

Figure 9-9.--Marking Guide for Publications and Correspondence.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

<p>* (U), (C), (S), (TS) (required for all paragraphs, subparagraphs, titles, headings, captions, etc). Naval Nuclear Propulsion Information (NNPI) will not be portion marked.</p>	<p>Critical Nuclear Weapons Design Information. DOD Directive S210.2 applies (Full Notice), CNWDI (Short form), (N) (Abbreviated form). Before each paragraph or portion (except NNPI), and before each caption. After headings and titles. (Use unclassified titles whenever possible to facilitate indexing.)</p>
<p>CLASSIFIED BY DOE-DOD classification guide CG-RN-1 dated January 1977. DECLASSIFY ON: Originating Agency's Determination Required. This document shall not be used as a derivative classification source (required marking for NNPI).</p>	<p>Once on covering (first) page.</p>
<p>WARNING NOTICES</p>	
<p>A RESTRICTED DATA This material contains Restricted Data as defined in the Atomic Energy Act 1954. Unauthorized disclosure subject to administrative and criminal sanctions (Full notice), RESTRICTED DATA (Short form), RD (Abbreviated form).</p>	<p>A Full notice at lower left on the covering (first page) beneath the "CLASSIFIED BY" line, in lieu of a "DECLASSIFY ON" line. Short form typed after classification at the top left on the first page of correspondence. Abbreviated form following portion marking classification symbol, e.g., (S-RD) or S-FRD).</p>
<p>FORMERLY RESTRICTED DATA Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, Atomic Energy Act of 1954 (Full notice), FORMERLY RESTRICTED DATA (Short form), FRD (Abbreviated Form).</p>	

Figure 9-9.--Marking Guide for Publications
and Correspondence..Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

INTELLIGENCE CONTROL MARKINGS	
WARNING NOTICE - INTELLIGENCE SOURCES OR METHODS INVOLVED (Full marking), WMINTEL (Short form), WN (Abbreviated form).	Full marking once at bottom center above classification marking on the front cover (if any), title page (if any) and first page of publication.
NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR CONSULTANTS (Full marking), NO CONTRACT (Short form), NC (Abbreviated form).	Full marking typed on the first page of correspondence following the classification at upper left.
CAUTION - PROPRIETARY INFORMATION INVOLVED (Full marking), PROPIN (Short form), PR (Abbreviated form).	Short form at top or bottom center of applicable pages, and for message classification lines, identification of tables, figures, charts, etc.
NOT RELEASABLE TO FOREIGN NATIONALS (Full marking), NOFORN (Short form), NF (Abbreviated form).	Abbreviated form following the classification designation in portion marking (e.g., (S-NC)).
THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO (Insert specified country(ies)) (Full marking), REL TO (Shortform), REL (Abbreviated form).	
DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (Full marking), OROON (Shortform), OC (Abbreviated form).	

Figure 9-9.--Marking Guide for Publications
and Correspondence..Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 10

ACCOUNTING AND CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	10000	10-3
PROCESSING INCOMING MAIL	10001	10-3
TOP SECRET DOCUMENTS	10002	10-4
TOP SECRET MESSAGES.	10003	10-5
SECRET MATERIAL.	10004	10-5
SECRET MESSAGES.	10005	10-6
CONFIDENTIAL INFORMATION	10006	10-6
CONFIDENTIAL MESSAGES.	10007	10-7
NAVAL WARFARE PUBLICATIONS	10008	10-7
SPECIAL HANDLING MESSAGES.	10009	10-7
CLASSIFIED MICROFICHE.	10010	10-8
CLASSIFIED ADP MATERIALS	10011	10-8
WORKING PAPERS	10012	10-8
CLASSIFIED MATERIAL IS NOT PERSONAL PROPERTY.	10013	10-9
TRANSFER ON RELIEF	10014	10-9
OTHER REQUIREMENTS	10015	10-9
REDUCTION/REVIEW OF CLASSIFIED MATERIAL	10016	10-9
INVENTORIES.	10017	10-10
PROCESSING OF COMMAND ORIGINATED CLASSIFIED MATERIAL.	10018	10-11
SECONDARY CONTROL POINT (SCP) ACCOUNTING AND CONTROL PROCEDURES	10019	10-11

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

FIGURE

10-1	RECORD OF DISCLOSURE.	10-13
10-2	CORRESPONDENCE/MATERIAL CONTROL SHEETS.	10-14
10-3	SAMPLE RECORD OF RECEIPT.	10-15
10-4	SAMPLE ACCESS LETTER FOR PERSONNEL AUTHORIZED TO RECEIPT FOR CLASSIFIED MATERIAL.	10-16
10-5	CHANGE ROUTE SHEET.	10-17

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 10

ACCOUNTING AND CONTROL

10000. BASIC POLICY. Classified information must be afforded a level of accounting and control commensurate with its assigned classification. Accounting and control serves to: Limit dissemination, prevent unnecessary reproduction, determine the office or person normally responsible for the material's security, and determine holders so they can be notified of unscheduled changes in the classification or compromise of the material. In the case of Top Secret information, it is also important to keep a current record of who has the information and who has seen it.

1. Processing of Incoming Material

a. The CMCC receives and routes all incoming classified material, except SSO/SAO material; personal correspondence for the Commander and Deputy Commander, electrical communications, FOCAL POINT material, and documents addressed to the AC/S G-2 or Counterintelligence Humint Office by NCIS which are marked "To be opened by the Commanding Officer Only."

b. All required administrative actions and forms for control of command classified material are executed at CMCC.

2. Use of Route/Locator Sheets

a. Changes in routing desired by divisions/sections concerned will be noted in the remarks section of the routing sheet and returned to CMCC for further routing. SCPs will not pass classified documents between SCPs.

b. Locator sheets will be signed by the individual picking up the material at the time of pick up and retained by CMCC personnel.

c. User divisions/sections will not remove the routing sheet that is attached to command controlled documents.

10001. PROCESSING INCOMING MAIL. Procedures must be developed within this headquarters to ensure that all incoming official mail, bulk shipments, and material delivered by messenger are adequately protected until a determination is made as to whether they contain classified material. The CMCC is the command screening point which ensures that incoming material is properly controlled and that access to classified material is limited to cleared personnel. Divisions and separate branches will designate an individual to open all official mail received by their division or branch. This

individual will possess a Secret clearance.

10002. TOP SECRET DOCUMENTS

1. The MARFORPAC TSCO, assisted by designated Top Secret control assistants, is responsible for receiving, maintaining accountability registers for and distributing Top Secret documents.
2. The TSCO will enter into this headquarter's accountability register all Top Secret documents originated or received by this headquarters for which the TSCO is responsible. The register will completely identify the Top Secret document including; changes, number of copies and give the disposition of each copy. The register will be retained for five years after the documents are transferred, downgraded or destroyed.
3. Serially number all copies of each Top Secret document and each item of Top Secret equipment at the time of origination in the following manner:

"Copy no. ___ of ___ copies."
4. Top Secret documents will contain a list of effective pages in which will be included a Record of Page Checks. When this is impractical, as in correspondence or messages, number the pages as follows:

"Page ___ of ___ pages."
5. The TSCO will page check Top Secret documents for completeness and accuracy on initial receipt and after entry of a change involving page entry or removal. (The change residue, including pages removed, must also be page-checked before destruction.) Page checks by the relieving officer, upon relief of the TSCO, are required.
6. Top Secret documents will be physically sighted or accounted for by examination of written evidence of proper disposition, such as certificate of destruction, transfer receipt, etc., at least once annually, and more frequently when circumstances warrant. At the same time, Top Secret records will be audited to determine completeness and accuracy.
7. Retention of Top Secret documents within this headquarters will be kept to a minimum. When Top Secret material is destroyed, CMCC will prepare a record of destruction identifying the material destroyed and the two officials who witnessed its destruction. The

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

10004

TSCO will reevaluate Top Secret command file copies which cannot be destroyed and, when appropriate, downgrade, declassify, or retire them to designated records centers.

8. All Top Secret material will be accounted for by a continuous chain of receipts. Hand-to-hand transfer with signed receipts is required for internal distribution of Top Secret, with a record kept of each individual to whom the information is disclosed.

9. The TSCO will maintain a disclosure record for each Top Secret document which shows the document title, name of all individuals, including stenographic and clerical personnel, who have been afforded access to the document, and the date of access. Retain disclosure records for two years after the documents are transferred, downgraded, or destroyed. OPNAV Form 5511/13 (Record of Disclosure (figure 10-1)) will be used for this purpose.

10. Top Secret material may not be reproduced without the consent of the originating agency or higher authority. The TSCO will serially annotate each copy reproduced.

10003. TOP SECRET MESSAGES. One copy of Top Secret messages, including Top Secret special handling messages, is received at the Force Command Center (FCC) via the SIH. The FCC will attach a Top Secret disclosure sheet to the message and forward this copy to the Staff Secretary for distribution instructions. The Top Secret disclosure sheet will be signed by each individual coming in possession of the message. The CMCC (Top Secret Control Officer/Assistant) will reproduce on pink paper, sufficient copies to make distribution as directed by the Staff Secretary. All residue and any excess copies will be destroyed. After initial distribution has been made, only the Staff Secretary and the TSCO may authorize reproduction of Top Secret messages.

1. Top Secret messages are on temporary loan to each division/section on distribution and will be returned to the TSCO when no longer needed.

2. The TSCO will maintain the command file for Top Secret messages.

10004. SECRET MATERIAL

1. The CMCC will establish administrative procedures for controlling Secret material to include records of material:

a. Originated or received by this headquarters.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

b. Distributed or routed to components of or activities within this headquarters.

c. Disposed of by this headquarters by transfer of custody or destruction.

2. Signed receipts are required for accountable Secret material distributed or routed within this headquarters. All Secret material transferred from one section to another within this headquarters will be routed through CMCC.

3. Figure 10-2, Correspondence/Material Control Sheets, will be attached to all Secret material under the control of CMCC within this headquarters.

4. When transmitting Secret material to another command, CMCC will enclose a receipt identifying the document(s). This receipt must be signed and returned to this headquarters regardless of the method of transmission. (See figure 10-3 for a sample receipt.) The Registered Mail receipt does not replace the Secret receipt. A Registered Mail receipt merely acknowledges that a package was received, it doesn't assure the sender that each piece of Secret material has been entered into the accountability system of the recipient. This headquarters is responsible for material until the addressee receives and signs for it. The CMCC cannot be sure that accountability has been transferred until the recipient signs the receipt and returns it.

10005. SECRET MESSAGES. Distribution of Secret messages, excluding special handling messages, will be made by the SIH. Due to the large volume of Secret messages, decentralized accounting procedures will prevail within this headquarters. The following procedures will be adhered to in the handling and control of Secret messages within divisions/sections:

1. SCPs will establish accounting procedures for each Secret message maintained.

2. SCPs are authorized to destroy Secret messages without record per CNO waiver to the current edition of OPNAVINST 5510.1. This does not pertain to Special Handling Messages mentioned in paragraph 10009 below.

10006. CONFIDENTIAL INFORMATION. Procedures for the protection of Confidential information are less stringent than those for Secret. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material, except for those messages listed in paragraph 10009 below and special handling

material such as NATO, etc., which will have correspondence material control sheets affixed. This excepted material must be returned to CMCC when no longer needed. Administrative provisions are required, however, to protect Confidential information from unauthorized disclosure by access control and compliance with the regulations on marking, storage, transmission, and destruction.

10007. CONFIDENTIAL MESSAGES. Distribution of Confidential messages, excluding special handling messages, will be accomplished by the SIH. SCPs will destroy Confidential messages when no longer needed. Destruction records are not required.

10008. NAVAL WARFARE PUBLICATIONS

1. Naval Warfare Publications (NWP), classified or unclassified, have their own system for administrative control. Classified NWPs are always to be handled and controlled as classified material first and NWPs second. In other words, the administrative controls for NWPs do not replace the security controls for classified material. All of the requirements of this regulation - access, accounting, storage, transmission, and destruction - must be adhered to for classified NWPs just the same as for any other classified material.

2. The NWP control officer is responsible to the Security Manager for accountability and control of classified NWPs.

10009. SPECIAL HANDLING MESSAGES. One copy of all messages requiring special handling to include; Special Category (SPECAT), Limited Distribution (LIMDIS), and Personal Fors (Secret and below) are received by the FCC and routed to the Staff Secretary for distribution instructions. The CMCC will reproduce sufficient copies to make distribution, except for "Personal Fors", which will be initially reproduced and distributed by the Staff Secretary. All residue/excess copies made during the reproduction of copies will be destroyed. After initial distribution has been made, only the Staff Secretary and the OIC CMCC may authorize the reproduction of special handling messages.

1. Special handling messages are under the control of CMCC and will be returned when no longer needed. Disposition instructions will be provided by the sections holding copies.

2. The OIC CMCC will maintain this headquarter's file copy for all special handling messages except that the Staff Secretary will maintain the headquarter's file copy of "Personal For" messages.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

3. SCPs will establish control procedures for these types of messages, to include receipt and disposition.

4. Special handling messages under the cognizance of the AC/S G-2 will be handled and controlled by that office only.

10010. CLASSIFIED MICROFICHE. In general, the policy and procedures for controlling classified documents apply equally to classified microfiche.

10011. CLASSIFIED ADP MATERIALS. Classified ADP storage media and output will be controlled and safeguarded in the same manner equivalent to that provided classified documents of a similar classification.

10012. WORKING PAPERS

1. Working papers are documents and material accumulated or created while preparing finished material. 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. Working papers will only be maintained for 90 days at which time they will be reviewed and if required to be maintained, made into a document.

b. Marked on each page with the highest classification of any information contained therein.

c. Protected per the classification assigned.

d. Destroyed by authorized means when no longer needed.

2. Follow the accounting, control and marking requirements prescribed for a finished document when working papers contain Top Secret information or are:

a. Released by this headquarters, transmitted electronically, or transmitted through message center channels within the command.

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

c. Filed permanently.

3. Waivers to the requirements to control Top Secret working papers within this headquarters will not be granted.

10013. CLASSIFIED MATERIAL IS NOT PERSONAL PROPERTY. Classified information is always official information and never personal property. Confusion sometimes arises about classified notes from a training course or conference. As classified material, they are official information which must be safeguarded, transmitted and destroyed per the guidance within this Manual. You cannot remove classified notes from this headquarters without the Security Manager's permission. Classified notes may be considered as working papers but, as official information for which this headquarters is responsible, they must be transmitted by means authorized for transmittal of classified material and eventually destroyed by authorized means. When individuals transfer from this headquarters, their notes may be officially transferred to the new command where they will again be available for use. When the individual is separated, released, or retired from the DON, all classified material must be turned in.

10014. TRANSFER ON RELIEF. Each SCP custodian and person about to be relieved will deliver to their successor all classified material in their custody. Appropriate receipts will be completed covering the change of custody for all Top Secret and CMCC accountable material. Classified material required by an individual at the next duty station, when approved by the losing command, may be officially transferred to the gaining command for the individual's use.

10015. OTHER REQUIREMENTS. Additional accounting and control requirements for special categories of classified material are contained in the current editions of the following directives:

1. COMSEC material - Cryptographic Security Policy and Procedures, CSP-1, and Communications Material Systems Manual (CMS-1).
2. NATO classified material - OPNAVINST C5510.101.
3. Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI) - OPNAVINST S5511.35.
4. Sensitive Compartmented Information - DOD C-5105.21-M-1.

10016. REDUCTION/REVIEW OF CLASSIFIED MATERIAL

1. Quarterly, CMCC and each SCP will conduct a review of all classified material maintained with the goal of reducing classified

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

holdings. Storage of classified material is costly and for this purpose, our holdings should be held to a minimum.

2. The results of this review will be reported to the Security Manager (AC/S G-1) by 15 August with a copy to CMCC.

10017. INVENTORIES

1. Inventories of all classified material controlled by CMCC will be held quarterly and prior to changing of the SCP Custodian. The results of all inventories will be routed to the OIC CMCC prior to relief by each respective SCP. Discrepancies in inventories will be reported to the Security Manager. SCP custodians will not transfer until discrepancies have been resolved.

2. A sight inventory of all Top Secret material (including working papers) held by CMCC and the SCPs will be conducted by the TSCO and witnessed by the Top Secret control assistant. This sighting will include an audit of each piece of material to determine completeness and accuracy of classification markings, serial numbers, related control data, and page checking.

a. On the first working day in March of each year, the TSCO will furnish each SCP with machine listings of all Top Secret material on temporary loan to that SCP.

b. The TSCO will report all discrepancies which cannot be resolved, to the Security Manager.

c. During the conduct of the sight inventory, SCP officers will review all classified holdings for that material which is no longer required. Such material will be returned to CMCC with disposition instructions noted on the routing sheet. During the sight inventory, any material found that is not under CMCC's control, will be sent to CMCC for accountability purposes.

3. An inventory of the Naval Warfare Publication Library (NWPL) publications will be held during August of each year by the NWPL Custodian and an appointed witnessing officer.

a. A listing will be provided to SCPs holding NWPL publications during August.

b. The listing will be returned to the NWPL custodian within two weeks of receipt, annotated to reflect all documents physically held, shortages, discrepancies, and certified as correct by the SCP custodian and a witnessing officer.

c. The Force Adjutant will cause the NWPL to be inspected during September and February of each year. The inspection will be conducted by an officer senior to the NWPL custodian. The results will be provided to the Force Adjutant by the inspecting officer within one week from the inspection date.

10018. PROCESSING OF COMMAND ORIGINATED CLASSIFIED MATERIAL

1. When in final form and ready for printing/distribution, classified material will be delivered to CMCC with reproduction and distribution instructions (see chapter 11). All copies shall be delivered to CMCC for accountability purposes. Working papers used in preparing the material will be destroyed by the originating division/section. Top Secret working papers will be turned in to the TSCO.
2. Any questions concerning administrative procedures for the preparation of classified material within this headquarters will be referred to the OIC CMCC for resolution.
3. The CMCC will receive, check for discrepancies, and prepare for mail or courier all classified material originated within this headquarters (less SSO). The OIC CMCC will return to the originating division/section for corrections, all classified material which does not conform to security or correspondence regulations.
4. The CMCC will maintain one copy of all command originated classified documents (less messages) as the command file copy. The command file copy will be maintained for five years.

10019. SCP ACCOUNTING AND CONTROL PROCEDURES. The accounting procedures discussed below are applicable to all SCPs and/or individuals that are custodians of classified material.

1. Before material classified Top Secret, NATO Secret or higher, or any classified JCS material may be received from CMCC by an authorized representative of an SCP, CMCC must obtain a receipt for each item of material. The receipts will be retained by CMCC.
2. SCP custodians will ensure that the "disposition" portion of route sheets are properly completed prior to returning them to CMCC.
3. To ensure prompt disposition of classified documents, divisions/sections will return copies of classified material requiring further routing to the CMCC within three working days after receipt. Divisions/sections desiring an extra copy or copies

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

will so annotate on the route sheet,

4. SCPs will not pass classified material between SCPs but will channel the material through the CMCC. An exception to this procedure is authorized for temporary loans of less than 10 days duration; however, nothing herein shall be construed as relieving either SCP from exercising appropriate accountability and control of temporarily loaned classified material.

5. SCP custodians will periodically review classified material on hand to ensure that such material is timely and pertinent to current requirements. Material that fail to meet the aforementioned criteria, will be destroyed or returned to the CMCC with complete disposition instructions.

6. SCPs are authorized to destroy all unclassified, Confidential and Secret messages, classified working papers (except Top Secret) and classified waste. All classified material which is Top Secret, NATO Secret and JCS material, regardless of classification, shall be returned to the CMCC for disposition.

7. The SCP custodian may authorize personnel to receipt for classified material. Once receipted for, this material becomes the responsibility of the SCP custodian. (See figure 10-4 for format.)

8. Changes to classified documents must be incorporated by the SCP having custody of the document, (except that Top Secret and special category material changes will be incorporated by CMCC). Changes will be issued to SCPs using a Change Route Sheet (see figure 10-5). Upon completion of the change, the SCP will return the change residue and the route sheet to CMCC for destruction. To ensure timely entry of changes, change route sheets will be returned to CMCC within three working days.

9. SCP custodians will establish a system for controlling their classified viewgraphs and magnetic tapes not under CMCC's control.

10. SCP custodians will ensure they review their access cards (located in CMCC) quarterly.

11. SCP custodians will ensure all persons check with their SCP files personnel when requesting classified material.

12. SCP custodians or their representatives will be the only personnel to contact CMCC for any material or problems dealing with classified material.

13. SCP custodians will ensure that classified material is picked up from CMCC on a daily basis.

**SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM**

<small>OPNAV 5517/10 (REV. 4-79) S/N 0107-LF-002-2300</small>		RECORD OF RECEIPT <small>(REFERENCE SECNAVINST 216.6)</small>				<small>THIS RECEIPT MUST BE SIGNED AND RETURNED.</small>
ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF MATERIAL	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF ENCL'S TO MAT'L REC'D	REGISTERED NUMBER

ADDRESS SEE (ACTIVITY RECEIVING MATERIAL)
SIGNATURE (AUTHORIZED RECEIPT)

DATE

MADE IN THE UNITED STATES OF AMERICA

Figure 10-3.--Sample Record of Receipt.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5510
2B
(Date)

MEMORANDUM

From: Assistant Chief of Staff, G-2
To: Staff Non-Commissioned Officer in Charge, Classified
Material Control Center

Subj: APPOINTMENT OF SECONDARY CONTROL POINT CUSTODIAN

Ref: (a) OPNAVINST 5510.1H
(b) MARFORPACO P5000.9B

1. The below listed individuals are appointed as Secondary Control Point Custodian and Alternates for the G-2 Division per the provisions of paragraph 2-11.5 of reference (a) and paragraph 5101.3c of reference (b). These individuals are authorized to receipt for classified material up to and including Top Secret.

Secondary Control Point Custodian

MGySgt John T. Jones 123 45 6789/0291

Alternate(s)

Sgt Mike M. Miller 123 45 6789/0151

2. Point of contact is MGySgt Jones at 477-0349.
3. This letter supersedes all previous authorizations.

J. D. LEATHERNECK
By direction

Figure 10-4.--Sample Access Letter for Personnel Authorized
to Receipt for Classified Material

**SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM**

CHANGE ROUTE SHEET

					CONTROL NUMBER	
DOCUMENT DATE	SERIAL NUMBER	TYPE	SSIC	DATE RECEIVED	COPY NO.	NO OF COPIES
ORIGINATOR						
SUBJECT						
		SUBJ CLASS	CHANGES	GUS	DISP & SECTION	

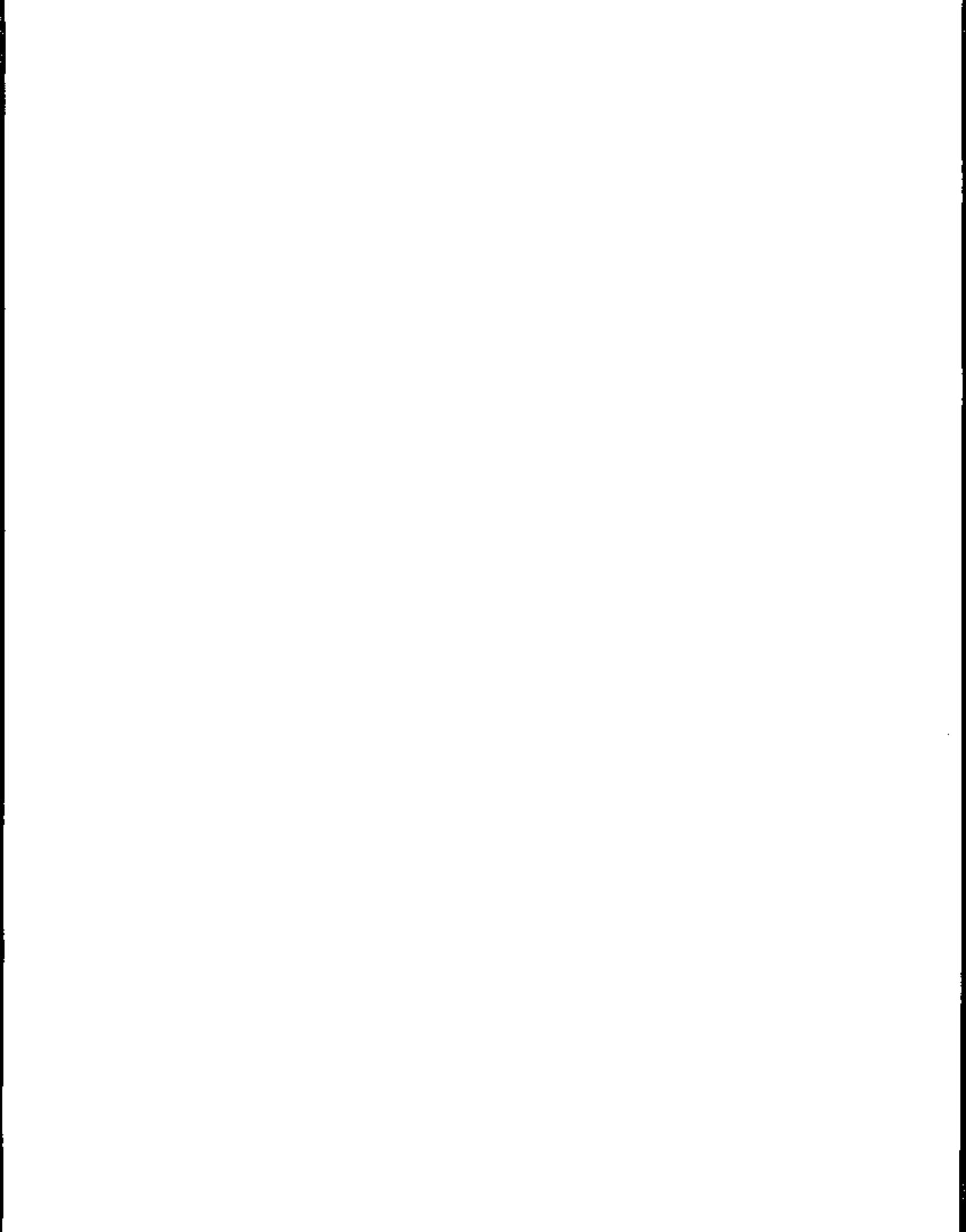
I certify that the above change or correction has been entered in the basic document, the list of effective pages was checked against the contents of the basic document, and the superseded pages and residue of the change were properly destroyed. In the event no residue exists, record that fact below in the remarks section.

<u> </u> (Section)	<u> </u> (Section)	Date
Witnessing Officer (Sgt & above)	Witnessing Officer (Sgt & above)	

Remarks: Return extra copies of changes with required distribution noted.

ROUTE SHEET TO BE RETURNED TO S&C AFTER COMPLETION

Figure 10-5.--Change Route Sheet.

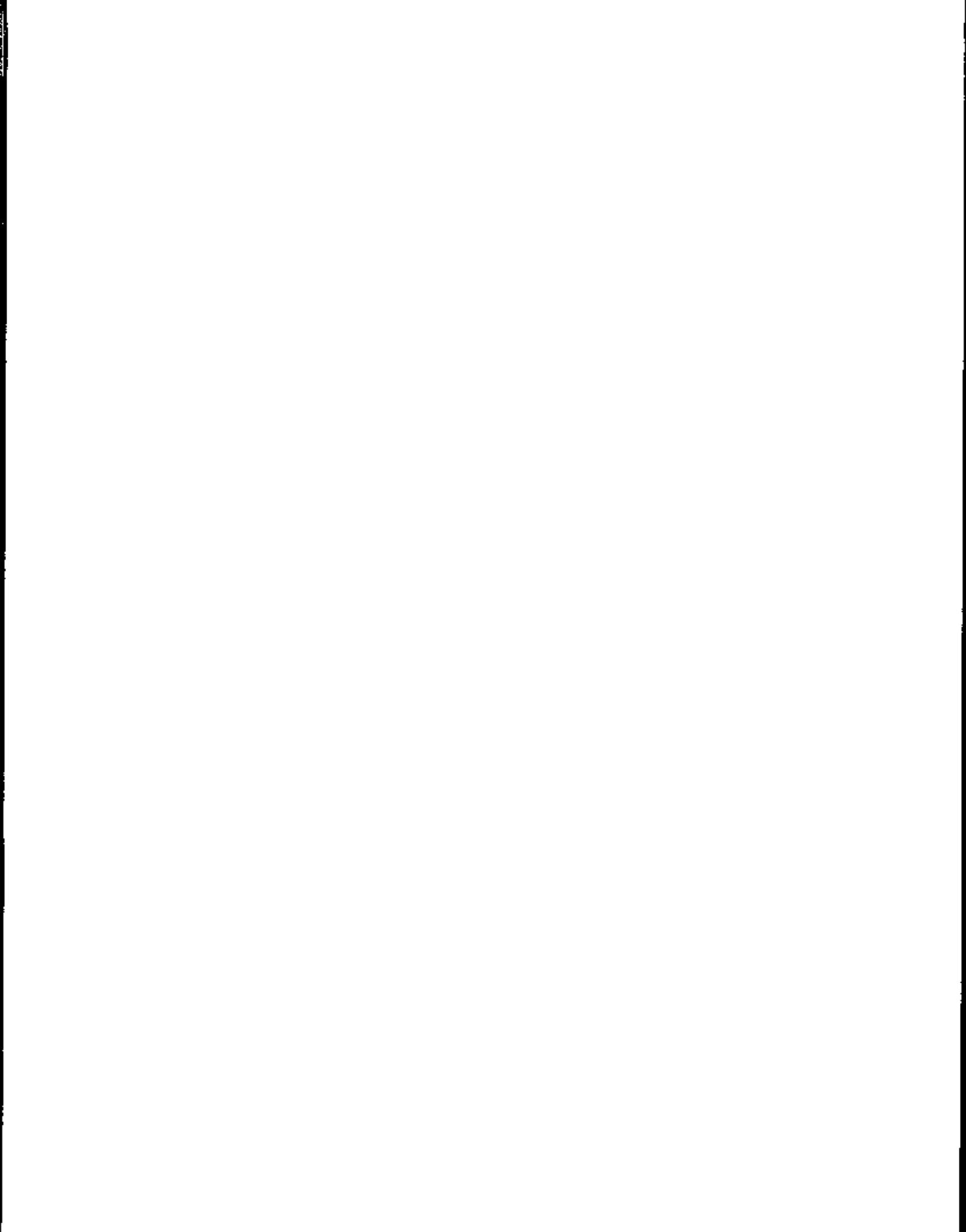


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	11000	11-3
CONTROLS ON PRINTING.	11001	11-3
CONTROLS ON REPRODUCTION.	11002	11-3
CONTROL OF PHOTOGRAPHY.	11003	11-4
CONTROL OF RECORDING SYSTEMS.	11004	11-4
TELECOPIERS/FACSIMILE MACHINES.	11005	11-5



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 11

PRINTING, REPRODUCTION AND PHOTOGRAPHY

11000. BASIC POLICY. The policy in this headquarters is to keep the reproduction of classified material to the absolute minimum while maintaining operational effectiveness. In order to accomplish this, controls exist within this headquarters concerning the printing, reproduction and photography of classified material.

11001. CONTROLS ON PRINTING. The Force Adjutant exercises responsibility for the printing of all classified material within this headquarters. All classified projects to be reproduced by the MARFORPAC Reproduction Branch, will be delivered to the CMCC to ensure the documents are correctly marked per chapter 9 of this Manual. Materials not properly marked will be returned to the requesting section for correction. The CMCC is the only section that can authorize the printing of classified information in the MARFORPAC Reproduction Branch. All printed copies of classified material will be returned to the CMCC for appropriate controls. Only Secret and Confidential material may be printed in the MARFORPAC Reproduction Branch. All Top Secret printing will be accomplished by the CMCC.

11002. CONTROLS ON REPRODUCTION. There are a number of reproduction machines within this headquarters that have not been authorized for the reproduction of classified material. The convenience of this reproduction equipment does not preclude obtaining the proper authorization needed for reproducing classified material. To limit the reproduction of classified material, the following rules apply:

1. All accountable classified documents will only be reproduced by the CMCC.
2. Top Secret material will not be reproduced except by the TSCO and only with the approval of the originator.
3. Sensitive Compartmented Information will only be reproduced by the SSO.
4. Secret and Confidential messages and working papers may be reproduced by divisions and separate branches upon inspection and approval of their reproduction equipment by the Security Manager. All divisions that have such reproduction equipment will designate an individual (E-6 or above) as an approval authority for all classified material reproduced within the division or branch. A

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

logbook will also be maintained to record the subject, date of material, date reproduced, individual reproducing the material, number of copies made, and the individual who authorized the reproduction of the material. Reproduction of classified material will be kept to a minimum.

5. All reproduction equipment authorized for reproducing classified material will be prominently marked as such. For example; "THIS MACHINE IS AUTHORIZED FOR REPRODUCTION OF CLASSIFIED MATERIAL UP TO AND INCLUDING SECRET." Reproduction must be approved by (Division/Branch Authorizing Official). All machines not authorized for the reproduction of classified material will have a warning notice. For example; "THIS MACHINE IS NOT AUTHORIZED FOR THE REPRODUCTION OF CLASSIFIED MATERIAL."

6. Reproduced material must contain the classification and other special markings which appear on the original material. All reproduced material should be checked and remarked if the markings are unclear.

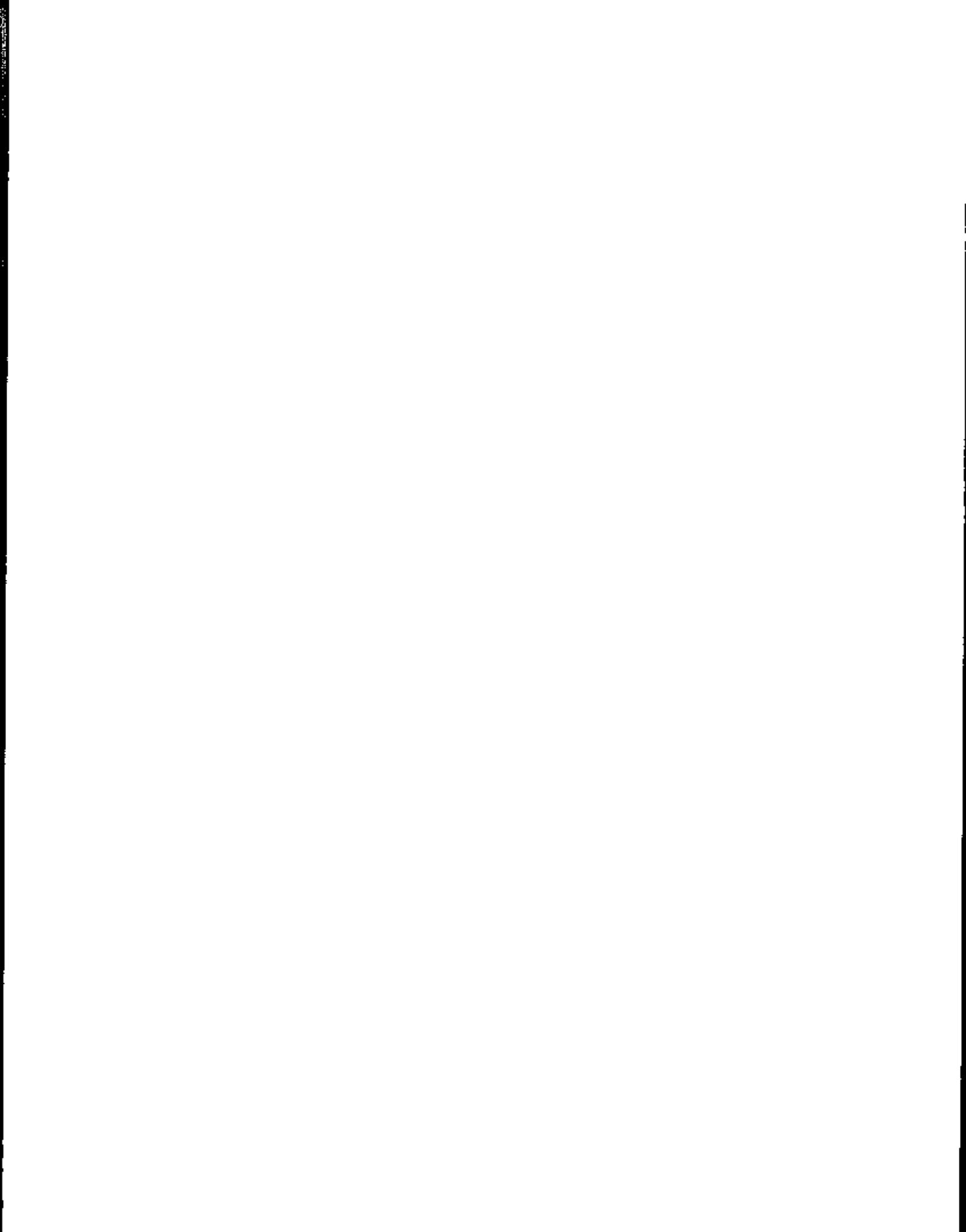
7. Samples, waste, or overruns resulting from the reproduction process, will be safeguarded according to the classification of the information involved. This material will be destroyed promptly as classified waste. Check areas surrounding reproduction equipment for classified material that may have been left on nearby desks or thrown in wastebaskets. In the event the machine malfunctions, check to ensure that all copies have been removed. After reproducing classified material, make sure the original and all copies have been removed from the machine.

11003. CONTROL OF PHOTOGRAPHY. All division and separate branch heads will ensure that only official photography is authorized in areas under their cognizance. Normally, such photography is used for events such as awards, promotions, and reenlistments. Steps will be taken to ensure that classified material is properly protected. All negatives will be inspected for evidence of classified information. Visitors will not be authorized to take photographs within this headquarters. Requests for the photography of classified materials will be provided to the TAVSU via the CMCC. Upon completion of the project, the materials will be returned to the CMCC for appropriate control based on the classification of the material.

11004. CONTROL OF RECORDING SYSTEMS. Personnel will not be allowed to bring voice recording equipment into areas where classified information is processed and discussed without approval of the Security Manager.

11005. TELECOPIERS/FACSIMILE MACHINES. The FCC has an authorized, secure telecopier/facsimile machine which can be used for the transmission of classified material up to and including Secret. Telecopiers and other similar devices using unsecured telephone lines, will not be used to transmit classified information, and all such machines will be prominently marked; "THIS EQUIPMENT IS NOT AUTHORIZED FOR THE TRANSMISSION OF CLASSIFIED INFORMATION." Those sections possessing an approved secured facsimile machine, will ensure that material faxed from this command is authorized by the section's SCP custodian and a record of traffic sent is maintained in a logbook for a minimum of two years. At the minimum, the logbook will contain:

1. Number material sent to.
2. Person receiving facsimile.
3. Date material sent.
4. Authorizing official.
5. Description of material sent; i.e., enclosure (1) of DIAM 5813, Vol II.

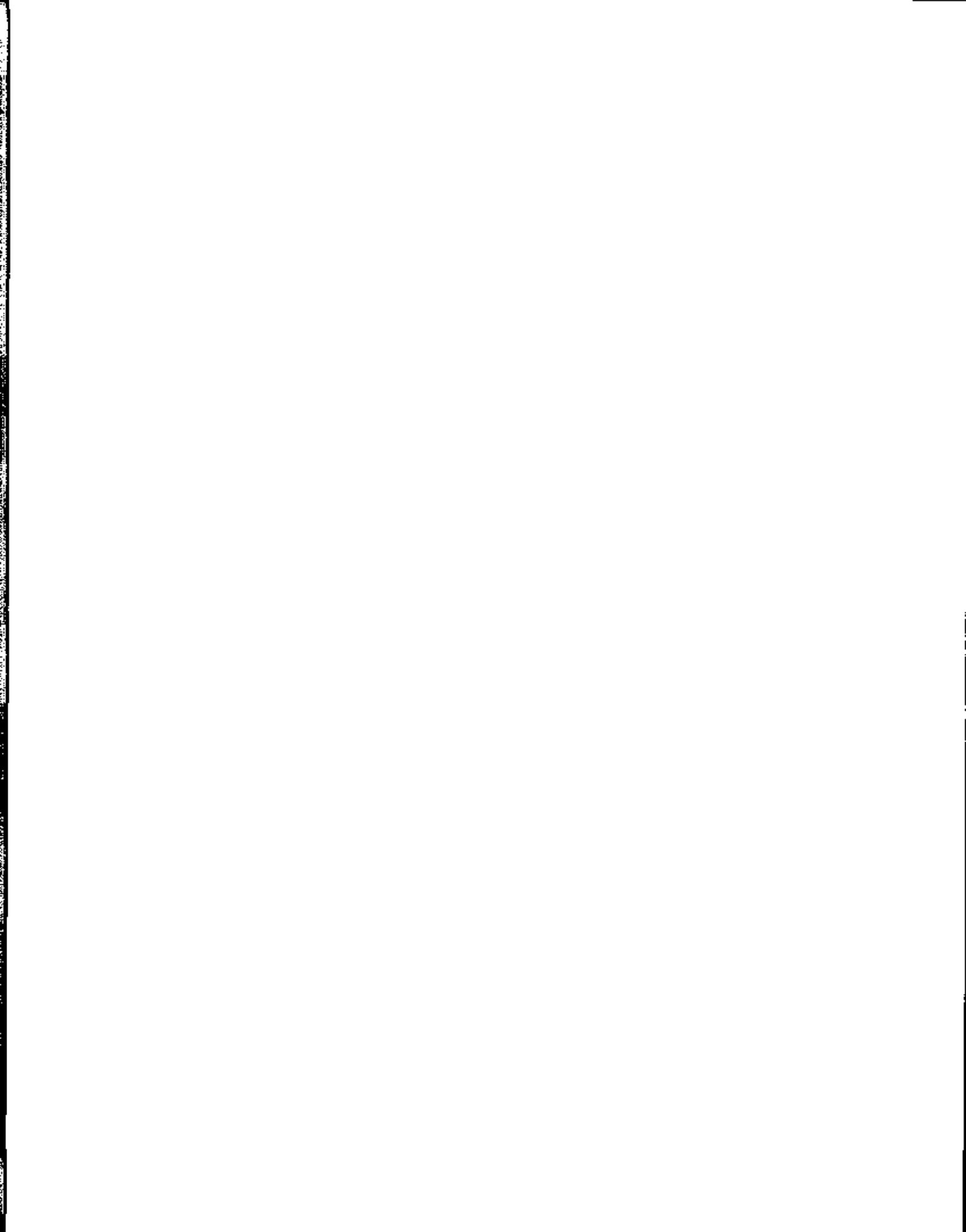


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	12000	12-3
RESTRAINTS ON SPECIAL ACCESS PROGRAMS . .	12001	12-3
MATERIAL ORIGINATED IN A NON-DOD DEPARTMENT OR AGENCY.	12002	12-3
RESTRICTED DATA AND FORMERLY RESTRICTED DATA	12003	12-3
NATO MATERIAL	12004	12-3
CRYPTOGRAPHIC INFORMATION	12005	12-3
TOP SECRET MATERIAL	12006	12-3
SECRET AND CONFIDENTIAL MATERIAL.	12007	12-4
DISSEMINATION TO CONTRACTORS.	12008	12-4
DISCLOSURE TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS	12009	12-4
DISSEMINATION OF INTELLIGENCE MATERIALS	12010	12-4
AUTHORIZED CONTROL MARKINGS FOR INTELLIGENCE INFORMATION.	12011	12-4
DISSEMINATION OF TECHNICAL DOCUMENTS. . .	12012	12-4



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 12

DISSEMINATION OF CLASSIFIED MATERIAL

12000. BASIC POLICY

1. Within this headquarters, the dissemination of classified material will be kept to a minimum consistent with operational requirements and based on the need to know principle.
2. All material prepared for public release will be delivered to the Security Manager for a security review per the current editions of SECNAVINST 5720.42 and MCO 5510.9.

12001. RESTRAINTS ON SPECIAL ACCESS PROGRAMS. Special access programs, other than those presently established, will not be imposed within this headquarters unless approved by the Security Manager.

12002. MATERIAL ORIGINATED IN A NON-DoD DEPARTMENT OR AGENCY. Non-DoD originated classified materials will not be distributed outside of the DoD without the approval of the originating department or agency.

12003. RESTRICTED DATA AND FORMERLY RESTRICTED DATA. Restricted Data and Formerly Restricted Data will only be disseminated per the provisions in the current edition of SECNAVINST 5510.28.

12004. NATO MATERIAL. NATO classified materials will only be disseminated per the provisions in the current edition of OPNAVINST C5510.101. Department of the Navy documents and documents originated by this headquarters which incorporate NATO information, will be disseminated per the current edition of OPNAVINST 5510.1 and this Manual.

12005. CRYPTOGRAPHIC INFORMATION. All cryptographic and CMS distributed information will be disseminated per the provisions of the current editions of CMS-1.

12006. TOP SECRET MATERIAL. All TOP SECRET material in this headquarters will only be routed from the TSCO to a SCP and returned to the TSCO. Top Secret material will not be routed from one SCP to another SCP.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

12007. SECRET AND CONFIDENTIAL MATERIAL. Secret and Confidential material, with the exception of working papers and messages, will not be permanently routed from one SCP to another SCP without being processed via the CMCC for appropriate accountability. An exception to this procedure is authorized for temporary loan of classified material not to exceed 10 days duration; however, nothing herein shall be construed as relieving either SCP from exercising appropriate accountability and control of temporarily loaned classified material. The borrowing SCP will not make copies of the material without processing the material through the CMCC.

12008. DISSEMINATION TO CONTRACTORS. Personnel in this headquarters are prohibited from discussing or releasing classified information and documents with contractors unless the visit has been approved by the Security Manager.

12009. DISCLOSURE TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS. Personnel in this headquarters will not discuss classified information with representatives of foreign governments or international organizations unless approved by the Security Manager. At no time will classified or unclassified documents be released to representatives of foreign governments or international organizations.

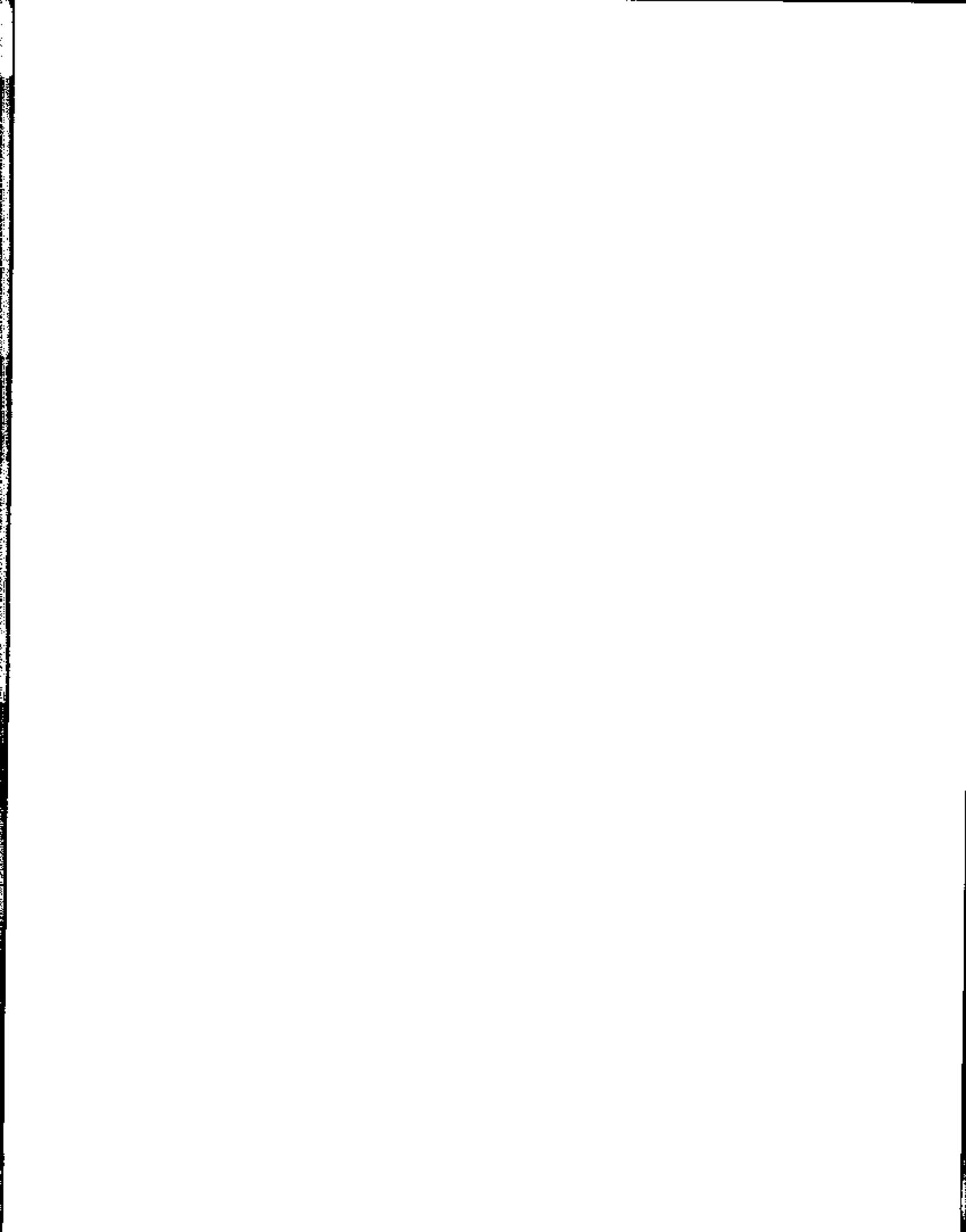
12010. DISSEMINATION OF INTELLIGENCE MATERIALS. The dissemination of intelligence materials within this headquarters will be controlled by the AC/S G-2. All requests for intelligence information will be provided/forwarded to the AC/S G-2 for appropriate action.

12011. AUTHORIZED CONTROL MARKINGS FOR INTELLIGENCE INFORMATION. The current and approved control markings for documents containing intelligence information are contained in chapter 12 of the current edition of OPNAVINST 5510.1.

12012. DISSEMINATION OF TECHNICAL DOCUMENTS

1. To reduce the risk of the undesired transfer of technical data with military applications, staff sections originating or responsible for technical documents must determine distribution limitations. All newly-generated classified and unclassified technical documents must bear one of the distribution statements described in exhibit 12B of OPNAVINST 5510.1H.

2. Distribution statements are not required to be placed on existing technical documents but may be applied, for the same reasons given in exhibit 12B of OPNAVINST 5510.IH, if the documents have not already been made generally available to the public.
3. Technical documents concerning cryptographic and communications security, communications and electronic intelligence, and other categories of information designated by the Director, National Security Agency (DIRNSA), are exempt from the provisions stated above, but must be approved by DIRNSA prior to public release.
4. Unclassified technical documents bearing a distribution statement will be given the same physical protection prescribed in the current edition of SECNAVINST 5720.42 "For Official Use Only" material.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 13

SAFEGUARDING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	13000	13-3
RESPONSIBILITY FOR SAFEGUARDING	13001	13-3
RESTRICTED AREAS.	13002	13-3
CLASSIFIED MATERIAL CONTROL CENTER (CMCC)	13003	13-4
SECONDARY CONTROL POINT (SCP)	13004	13-5
SUB-CUSTODY CONTROL POINT (SCCP).	13005	13-6
USCINCPAC SECURITY BADGES	13006	13-6
CARE OF WORKING SPACES.	13007	13-7
TECHNICAL SURVEILLANCE COUNTERMEASURES SERVICES.	13008	13-7
TEMPEST SERVICES.	13009	13-8
CARE DURING WORKING HOURS	13010	13-8
SAFEGUARDING FOREIGN OR INTERNATIONAL PACT ORGANIZATION INFORMATION	13011	13-9
SECURITY CHECKS	13012	13-9
SECURITY INSPECTIONS AND REVIEWS.	13013	13-10
SAFEGUARDING IN AN EMERGENCY.	13014	13-12

FIGURE

13-1	COVER SHEET FOR CLASSIFIED MATERIAL.	13-15
------	---	-------

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

13-2	SAMPLE PROCEDURES FOR SECURITY CHECKS	13-18
13-3	CLASSIFIED CONTAINER CHECK-OUT SHEET	13-20
13-4	SECURITY CHECK-OUT SHEET.	13-21

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

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. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. Security requirements must permit the accomplishment of essential functions while affording classified information appropriate security. The requirements specified in this Manual represent the minimum acceptable standards.

13001. RESPONSIBILITY FOR SAFEGUARDING

1. Anyone in possession of classified material is responsible for safeguarding it at all times, and particularly for locking classified material in appropriate security equipment whenever it is not in use or under the direct supervision of authorized persons. The custodian must follow procedures which ensure that unauthorized persons do not gain access to classified information by sight, sound or other means. Classified information will not be discussed with or in the presence of unauthorized persons.

2. Individuals will not remove classified material from designated offices or working areas except in the performance of their official duties and under conditions providing the protection required by this Manual. Under no circumstances will a custodian remove classified material from designated areas to work on it during off duty hours, or for any other purpose involving personal convenience.

13002. RESTRICTED AREAS

1. Different areas within this headquarters may have varying degrees of security importance depending upon their purpose and the nature of the work, information and materials concerned. To meet this situation requires the application of protective measures commensurate with these varying degrees of security importance.

2. To provide for an effective and efficient basis for applying the varying degrees of restricted access, control of movement, and type of protection required for classified information, the following applies to restricted areas:

a. Level Three (Formerly Exclusion Area). An area containing

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 14

STORAGE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	14000	14-3
STORAGE REQUIREMENTS.	14001	14-3
SECURITY CONTAINERS	14002	14-3
VAULTS AND STRONGROOMS.	14003	14-4
COMBINATION LOCKS AND COMBINATIONS.	14004	14-4
KEY CONTROL	14005	14-5
ELECTRICALLY ACTUATED LOCKS	14006	14-5
SECURITY CONTAINER DOCUMENTATION.	14007	14-5
SECURING SECURITY CONTAINERS.	14008	14-6
REPAIRING SECURITY CONTAINERS	14009	14-6
INTRUSION DETECTION SYSTEMS (ALARMS).	14010	14-6

FIGURE

14-1	COMBINATION CHANGE ENVELOPE.	14-7
14-2	CLASSIFIED CONTAINER INFORMATION	14-8
14-3	CLASSIFIED CONTAINER CHECK-OUT SHEET	14-9
14-4	PROCEDURES FOR SECURING SECURITY CONTAINERS	14-10

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 14

STORAGE

14000. BASIC POLICY

1. Division and separate branch heads are responsible for safeguarding all classified information under their cognizance. This includes ensuring that it is stored in the manner prescribed in this chapter when it is not being used or is not under the personal observation of cleared persons.
2. Report any weakness or deficiency in equipment used to safeguard classified material in storage to the Security Manager.
3. Do not store valuables, such as money, jewels, precious metals, narcotics, etc., in the same containers used to safeguard classified material. They increase the risk of a container being opened or stolen, with the resulting compromise of the information in it.
4. For identification purposes in the event of emergency destruction or evacuation, place a number or symbol indicating relative priority on the exterior of each security container (i.e., A or I equals Priority I, B or II equals Priority II, and C or III equals Priority III). The external markings will not indicate the level of classified information stored in the container.

14001. STORAGE REQUIREMENTS. All classified material will be secured in a General Services Administration (GSA) approved security container or a certified vault or strongroom. Open storage of classified material is not permitted unless the Security Manager has specifically authorized such storage in writing. Top Secret material will be stored in such a manner as to preclude lone access to that material. Top Secret material will not be openly stored in strongrooms.

14002. SECURITY CONTAINERS. Security containers will not be requested or procured until a requirement has been validated and approved by the Security Manager. All requests for security equipment such as alarms, shredders, security containers and locking devices will be processed via the Security Manager. The Security Manager will maintain security container records forms (OPNAV Form 5510/21) for all security containers. New security equipment will not be placed into service until it has been inspected by CI personnel.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

14003. VAULTS AND STRONGROOMS. Certain divisions and separate branches have certified vaults and strongrooms. Open storage in a strongroom after completion of a CI physical security evaluation must be approved in writing by the Security Manager. All work requests for the construction of vaults and strongrooms will be coordinated with the Security Manager and the information provided to the Facilities Officer, Camp H. M. Smith for review. The work request will then be forwarded to the Facilities Office, MCBH.

14004. COMBINATION LOCKS AND COMBINATIONS

1. Only certified combination locks will be used in conjunction with the securing of classified material. The Security Manager maintains a list of approved combination locks which may be used.

2. Combinations will only be changed by trained personnel. A lockout, as a result of an untrained individual attempting to change a combination, could result in administrative action. Combination changes and other container maintenance will be accomplished by providing a DD Form 1149 (Open Purchase Request) to HQSVCBn Supply who will in turn contract the work out to a commercial vendor. CI personnel are available to train SCP personnel in the proper procedures for changing combinations and to perform limited maintenance on an emergency basis only.

3. To help ensure the effectiveness of combination locks, the following requirements apply:

a. Allow only individuals cleared for the highest level of classified material in the container to change combinations.

b. Give the combination only to those whose official duties demand access to the container.

c. Change combinations when placed in use, at least annually thereafter, and when any of the following occurs:

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

(2) The combination has been compromised or the security container has been discovered unlocked and unattended.

(3) The container (with built-in lock) or the padlock is taken out of service. Reset built-in combination locks to the standard combination 50-0. Reset combination padlocks to the standard combination 25-0.

d. In selecting combination numbers, do not use multiples of 5, simple ascending or descending arithmetical series or personal data such as birth dates and serial numbers.

e. Do not use the same combination for more than one container in any one section.

f. In setting a combination, use numbers that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

g. To prevent a lockout, have two different people try a new combination before closing the container or vault door.

h. Assign to the combination of a vault or container, a security classification equal to the highest category of the classified material authorized to be stored in it.

i. Seal records of combinations in an envelope (OPNAV Form 5511/2, figure 14-1). The envelopes containing TOP SECRET and SECRET combinations to the master container, will be stored in the FCC after the appropriate control procedures have been implemented by the CMCC. The recording of combinations will be done immediately after the combinations have been changed.

14005. KEY CONTROL. Division and branch heads will ensure that keys to all offices are maintained within the FCC. This may be a master key to a key box in a central location within the division or branch.

14006. ELECTRICALLY ACTUATED LOCKS. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford the degree of protection required for classified information. These locks are used for the sole purpose of limiting access to a specific area and are not authorized to be used to safeguard classified material.

14007. SECURITY CONTAINER DOCUMENTATION. All security containers, vaults and strongrooms will have the following documentation attached in a conspicuous manner.

1. OPEN and CLOSED sign.

2. Classified Control Information Form (OPNAV 5511/30) showing the names of all persons having knowledge of the combinations. Figure 14-2 indicates the proper method of completing this form.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

classified information which is of such a nature that unauthorized access to the area would cause GRAVE DAMAGE to the mission or national security. Only persons whose duties actually require access and who have been granted the appropriate security clearance will be allowed into Level Three areas.

b. Level Two (Formerly Limited Area). An area containing classified information and in which uncontrolled movement would permit access to classified information which would cause SERIOUS DAMAGE to the command mission or national security if compromised. All persons admitted to a Level Two area with freedom of movement must have an appropriate security clearance. Persons who have not been cleared for access to the information contained within a level two area may, with appropriate approval, be admitted to the area but they must be controlled by an escort, attendant or other security procedures to prevent access to classified information.

c. Level One (Formerly Controlled Area). An area within which uncontrolled movement will not permit access to classified information, and if compromised, would cause DAMAGE to the command mission and national security. This area is designed for the principal purpose of providing administrative control, safety or a buffer area of security restriction for limited or exclusion areas.

3. Level One, Two and Three areas will not be designated in any way that outwardly notes their relative sensitivity. Identify any such area as a "Restricted Area." Signs for restricted areas are available from the Security Manager.

4. All offices in this headquarters which store, process or discuss classified information will be conspicuously marked as a "Restricted Area" and will conform to the standards of a Level One area as defined above.

13003. CLASSIFIED MATERIAL CONTROL CENTER (CMCC)

1. The CMCC is the central repository for all classified material received, originated or transmitted within this headquarters. The CMCC is responsible for the following:

a. Accountability, routing, inventories, downgrading/declassification and destruction of all Top Secret and Secret materials, excluding Secret messages.

b. All Naval Warfare Publications. (NOTE: NWP's will be controlled and maintained by the CMCC.)

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

classified information which is of such a nature that unauthorized access to the area would cause GRAVE DAMAGE to the mission or national security. Only persons whose duties actually require access and who have been granted the appropriate security clearance will be allowed into Level Three areas.

b. Level Two (Formerly Limited Area). An area containing classified information and in which uncontrolled movement would permit access to classified information which would cause SERIOUS DAMAGE to the command mission or national security if compromised. All persons admitted to a Level Two area with freedom of movement must have an appropriate security clearance. Persons who have not been cleared for access to the information contained within a level two area may, with appropriate approval, be admitted to the area but they must be controlled by an escort, attendant or other security procedures to prevent access to classified information.

c. Level One (Formerly Controlled Area). An area within which uncontrolled movement will not permit access to classified information, and if compromised, would cause DAMAGE to the command mission and national security. This area is designed for the principal purpose of providing administrative control, safety or a buffer area of security restriction for limited or exclusion areas.

3. Level One, Two and Three areas will not be designated in any way that outwardly notes their relative sensitivity. Identify any such area as a "Restricted Area." Signs for restricted areas are available from the Security Manager.

4. All offices in this headquarters which store, process or discuss classified information will be conspicuously marked as a "Restricted Area" and will conform to the standards of a Level One area as defined above.

13003. CLASSIFIED MATERIAL CONTROL CENTER (CMCC)

1. The CMCC is the central repository for all classified material received, originated or transmitted within this headquarters. The CMCC is responsible for the following:

a. Accountability, routing, inventories, downgrading/declassification and destruction of all Top Secret and Secret materials, excluding Secret messages.

b. All Naval Warfare Publications. (NOTE: NWP's will be controlled and maintained by the CMCC.)

c. NATO. All personnel who require access to NATO information must be briefed on NATO security procedures by the CMCC before access is granted.

2. The CMCC will establish and maintain effective control procedures for accountability of all Top Secret and Secret material (less Secret messages) routed within this headquarters.

13004. SECONDARY CONTROL POINT (SCP)

1. SCPs are administrative extensions of the CMCC established to permit access to readily used classified materials by cognizant action officers.

2. A SCP is designated in writing (by the Security Manager) as a classified material storage area which draws classified material from the CMCC.

3. Divisions/sections having designated SCPs may hold classified material overnight, provided the following requirements have been accomplished:

a. The section meets the minimum physical security requirements as established by a counterintelligence physical security evaluation (PSE). Initial counterintelligence evaluations will be conducted by the MARFORPAC Counterintelligence Humint (CIH) personnel upon written request addressed to the Security Manager. Subsequent evaluations will be conducted by the SCP custodian and forwarded to the MARFORPAC Security Manager for approval. At a minimum, reevaluations will be conducted every two years or when security standards are changed or modified. NOTE: A new evaluation is required each time security containers are relocated from one office space to another.

b. Sections maintaining classified material will establish a control system for all classified material. In addition, divisions and branches will appoint a primary SCP custodian and an alternate SCP custodian, per paragraph 2001 of this Manual.

c. Divisions/sections not having an SCP must return all classified material to the CMCC by 1600 each day.

4. SCPs are responsible to the CMCC for all Top Secret and Secret documents (less Secret messages) received within their division or separate branch.

5. SCPs will only be established as considered necessary and will not be established as a matter of convenience. SCPs will be kept to an absolute minimum consistent with operational requirements.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

6. If a SCP is not used on a daily basis, the need for the SCP is questionable and a recommendation will be made to the Security Manager for disestablishment.

13005. SUB-CUSTODY CONTROL POINT (SCCP)

1. SCCPs are administrative extensions of a SCP. SCCPs are responsible to the SCP for all Top Secret and Secret documents (less Secret messages).
2. SCCPs will be kept to an absolute minimum.
3. All SCCPs will be the subject of a physical security evaluation by counterintelligence personnel. The Security Manager must approve (in writing) the establishment of a SCCP prior to the storage of classified material.
4. If a SCCP is not used on a daily basis, a recommendation will be made to the Security Manager for disestablishment.

13006. USCINCPAC SECURITY BADGES

1. Security Badges. Certain MARFORPAC personnel require a badge for entry into the USCINCPAC Command Center. The badge is issued for a maximum period of three years and authorizes access to the USCINCPAC Command Center, Intelligence Pacific (IPAC), MARFORPAC SCI facility and certain areas therein.
2. Requirements. The requirements for a USCINCPAC Command Center Badge are; that the individual requesting for the badge has a certified need for access to the USCINCPAC Command Center, SI/SAO access within MARFORPAC and is filling a designated SI/SAO billet.
3. Issue of Security Badges. Badges will be issued on a case-by-case basis at the time of indoctrination at the MARFORPAC SSO.
4. Security Badge Accountability. USCINCPAC Command Center badges are accountable and must be returned to the SSO upon expiration, when no longer required, or upon transfer of the holder from MARFORPAC. The loss or theft of a badge must be reported to the Security Manager immediately.
5. Wearing of Badges. USCINCPAC badges must be worn fully exposed while within the USCINCPAC Command Center. Upon departure from the facility, the badge must be removed or otherwise placed in a location where it is not visible.

6. The essential point to remember is, coded cards and badges are only an aid for determining the current level of personnel security clearance of the holder to the closed or restricted areas to which the holder may have access. They may not be used as the basis for granting access to information or areas.

13007. CARE OF WORKING SPACES

1. All office spaces containing classified information, should be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified information, specifically including security measures to prevent persons outside the building or spaces from viewing or hearing classified information.

2. All office spaces where classified material is stored, processed or discussed should be sanitized when uncleared personnel are performing repairs, routine maintenance or cleaning. These individuals will be escorted at all times and all individuals will be alerted to their presence.

3. Ensure adequate controls are established to prevent unauthorized individuals from being exposed or gaining access to exposed areas where classified material is adrift.

4. Extraneous material (such as unclassified papers, ADP printouts, publications) should be kept off the tops of security containers to prevent inadvertent intermingling of classified with unclassified material.

5. Burn bags will not be collocated adjacent with trash receptacles as the subconscious act of discarding waste material could result in classified material being discarded with regular trash.

13008. TECHNICAL SURVEILLANCE COUNTERMEASURE SERVICES. Technical Surveillance Countermeasures Services (TSCM) are available to this headquarters for the purpose of detecting any attempts to obtain classified information from this headquarters through the use of clandestine listening devices. All TSCM services will be requested through the Security Manager. A request will be classified Secret. To minimize the technical threat, the following principles will be applied within this headquarters:

1. Telephones, office intercommunications or public address systems will not be permitted in conference rooms except those amplifiers and simultaneous translation facilities essential to the meeting which have been checked to ensure that no intelligible signal is radiated beyond the limits of the secure area.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

2. In all offices in which classified information is discussed, personnel from the office will conduct frequent and thorough inspections of the spaces for unauthorized wiring and possible concealment of listening devices. Personal radios, TVs or recording devices are not allowed in classified discussion areas. Make sure any equipment in the area is dedicated to the facility and not introduced from outside for specific classified presentations.

3. If a suspicious device or unauthorized wiring is suspected, the Security Manager will immediately be notified. Do not touch or tamper with such a device. The telephone will not be used to make the report. All reports will be made in person.

13009. TEMPEST SERVICES. TEMPEST inspections will be conducted on all electrical equipment used to process classified information. These inspections detect whether or not compromising emanations are emanating from such equipment. TEMPEST inspections are requested from and conducted under the cognizance of the Assistant Chief of Staff, G-6. All requests for TEMPEST inspections will be classified CONFIDENTIAL and will be provided to G-6 with an information copy to the Security Manager per the current edition of MARFORPACO 5510.17.

13010. CARE DURING WORKING HOURS. During working hours, all offices shall establish precautions to prevent access to classified information by unauthorized persons:

1. Classified documents removed from storage for working purposes, will be kept under constant surveillance. Classified material cover sheets, such as OPNAV Form 5216/96 (figure 13-1), or MARFORPAC classified document folders may be used for this purpose.

2. Discuss classified information only when unauthorized persons cannot overhear the discussion. Take particular care when there are visitors or workmen present. Escorts should alert fellow workers when visitors or workmen are in the area.

3. Protect preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets and all similar items containing classified information either by destroying them by a method approved for destroying classified material immediately after they have served their purposes, or by giving them the same classification and safeguarding them in the same manner as the classified material they provided.

4. Classified typewriter ribbons should be protected/destroyed the same as the highest level of classification for which used. Exceptions are:

a. After the upper and lower sections have been cycled through the machine five times in the course of regular typing, all fabric ribbons may be treated as unclassified even if they are used subsequently for classified.

b. Typewriter ribbons which remain substantially stationary in the typewriter until it has received at least five consecutive impressions, may be treated as unclassified ribbon.

5. Typewriters which incorporate a non-removable/non-volatile internal magnetic memory device, will not be used for the preparation of classified material unless the equipment is protected according to the highest classification of material recorded in the memory device.

6. During lunch hours, all offices which have classified material adrift will be under the constant surveillance of cleared personnel. Locking the office door with classified material adrift and leaving the area constitutes a security violation and will be handled accordingly.

13011. SAFEGUARDING FOREIGN OR INTERNATIONAL PACT ORGANIZATION INFORMATION

1. Provide classified information of foreign origin the same protection as U.S. information of equivalent classification. Protect Foreign Restricted, for which there is no U.S. equivalent, the same as U.S. CONFIDENTIAL.

2. Do not intermingle NATO classified documents with U.S. documents in storage containers. NATO documents may be filed in the same drawer of a security container with U.S. documents if segregated and clearly identified as NATO files. The current edition of OPNAVINST C5510.101, contains additional guidance on protecting NATO classified material.

13012. SECURITY CHECKS

1. Division and separate branch heads will require a security check at the end of each working day to make sure all classified material is properly secured.

2. Sample procedures for security checks are contained in figure 13-2. Those conducting security checks will make sure that:

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

- a. All classified material is properly stored.
 - b. Burn bags are properly stored or destroyed.
 - c. The contents of wastebaskets which contain classified material have been properly stored or destroyed.
 - d. Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.
 - e. Security containers have been locked by the responsible custodian. Classified container check-out sheets (figure 13-3) will be used as a record of security container securing and double checks. (The dial of combination locks will be rotated at least four complete times in the same direction when securing safes, files or cabinets.)
3. A double security check will be conducted of all offices that store and process classified information. The office security check will be conducted by two individuals and recorded on a security check-out sheet as identified in figure 13-4.
4. If offices are accessed after a security check has been conducted, then another security check will be performed and recorded on the security check sheet.

13013. SECURITY INSPECTIONS AND REVIEWS

1. Secondary Control Point Inspection:

- a. The CMCC will conduct annual administrative inspections of each SCP and branches/sections authorized to store classified material.
- b. The results of this inspection will be provided to the AC/S G-1 (Security Manager).

2. Unannounced Counterintelligence Inspections:

- a. Unannounced counterintelligence inspections (UCIs) will be conducted on a quarterly basis. These inspections will be conducted both during and after normal working hours. The purpose of these inspections is to check for classified material left adrift and to ensure compliance with this Manual and the current edition of OPNAVINST 5510.1.

b. Each section within MARFORPAC will assign one individual (recommend the SCP custodian) with a Top Secret clearance, to assist in the conduct of UCIs. During the conduct of the UCI, one representative from the CIHO and three individuals will assist in the conduct of the inspection under the cognizance of the Security Manager.

(1) CI personnel are issued counterintelligence credentials by Headquarters, U. S. Marine Corps and will display them upon request. These credentials will be accepted as sufficient identification and additional identification is not required, unless exceptional circumstances exist. All CI Marines within this headquarters possess a Top Secret security clearance based on an SBI/SSBI.

(2) CI personnel are granted access to classified material up to and including Top Secret in the performance of official duties. As such, they are authorized unescorted access to all working spaces within this headquarters in the performance of official duties. CI personnel are also authorized to receipt for keys to all offices from the FCC.

c. Prior to the commencement of an after working hours UCI, the inspection team will report to the FCC and receipt for keys to the offices concerned. The following additional information is provided:

(1) CI inspectors are authorized to unlock and open for inspection such furnishings as desks, file cabinets, lockers, briefcases or other such containers not designed for storage of classified material.

(2) In addition, CI inspectors are authorized to recall responsible individuals to unlock security areas with combination locks and rooms for which keys are not available in the FCC.

(3) CI inspectors will also check typewriters, memory devices and word processing equipment for the purpose of determining whether or not they contain classified information.

d. The inspection team will provide the results of UCIs to the CDO. A written report will be provided the following working day for all security inspections.

e. Offices which are the subject of a security violation, will be reinspected within 30 days to determine whether corrective action has been instituted to increase security awareness and to ensure proper procedures outlined in this Manual are being complied with.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

f. Unannounced random personal security inspections are authorized to be conducted of all persons departing this headquarters, to determine if classified material is being removed from the building. Such inspections will include personal articles such as packages, parcels, purses, handbags, brief cases or similar containers. Any individual departing this building who refuses inspection of personal articles will be detained and the matter will be referred to the Security Manager.

13014. SAFEGUARDING IN AN EMERGENCY. The responsibilities for safeguarding classified material in the event of an emergency situation are set forth below:

1. Camp Commander, Camp H. M. Smith:

a. Depending upon the severity of the damage caused by any natural phenomena, e.g., fire, explosion, structural failure or similar causes, the Camp Commander shall be prepared to deploy a perimeter guard force at the affected area(s). Personnel who constitute this guard force will receive periodic instructions on procedures necessary to prevent removal of classified material by unauthorized personnel.

b. Classified material in the affected area(s) will be removed only through control points designated by the Camp Commander, Security Manager or the senior officer present. Only those persons designated will be authorized to remove classified material.

c. The Camp Commander will assign guards to protect classified material while it is in transit to the area designated for temporary stowage. If adequate security personnel cannot be provided at the temporary stowage area, the Camp Commander will also provide a guard force at the stowage area.

2. Security Manager:

a. Is responsible for effecting liaison with the Camp Commander concerning a guard force and transportation for the classified material to the temporary stowage area.

b. Is responsible for the designation of temporary stowage areas for the classified material removed from the affected area.

c. Remains responsible for the classified material while it is being removed from the affected area and transported to the temporary storage area.

d. Will notify the Commander or senior officer present upon completion of the relocation of the classified material.

3. Division and Separate Section Heads. Each division and separate section will prepare detailed emergency plans to meet specific requirements. Primary consideration should be given to fire, loss of essential services and structural failure; however, plans for emergency care should also provide for emergency action in any given situation.

TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION
(ORANGE)

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

TOP SECRET

703-101
NSN 7540-01-213 7901

STANDARD FORM 703 (8 85)
Prescribed by GSA/1500
32 CFR 2003

Figure 13-1.--Cover Sheet for Classified Material.

SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION
(RED)

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT
IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL
SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED
DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE
ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

SECRET

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)
Prescribed by GSA/1500
32 CFR 2003

Figure 13-1.--Cover Sheet for Classified Material..
Continued

CONFIDENTIAL

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION
(BLUE)

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT
IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL
SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED
DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE
ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

CONFIDENTIAL

705-101
NSN 7540-01-213-7903

STANDARD FORM 705 (8-65)
Prescribed by GSA/1900
32 CFR 2003

Figure 13-1.--Cover Sheet for Classified Material.--
Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SAMPLE PROCEDURES FOR SECURITY CHECKS
AT THE END OF THE WORKING DAY

1. All individuals must be sure their working areas are secure at the end of the working day by:
 - a. Looking on top, under, behind or in desks and removing and securing all classified material.
 - b. Making sure that working trays and baskets are empty.
 - c. Properly storing and shredding notes, carbons, roughs drafts and similar working papers.
 - d. Placing classified documents, correspondence or related classified material in proper security containers.
 - e. Removing disks and printer ribbons from word processors and PCs and making sure the electrical power is turned off.
 - f. Securely closing and locking each drawer or door of security containers and rotating the dials at least four complete turns in the same direction.
 - g. Surveying the general area to be sure no classified material is unsecured. This includes all trash containers.
2. Each week a staff member will be assigned responsibility for double checking the spaces to ensure that they have been secured, using the daily security checklist. Each item will be checked and initialed. The double checklist will ensure:
 - a. All security containers in the area are closed and locked by rotating the combinations locks four times in the same direction and trying the locking drawer.
 - b. The reproduction machine is cleared by running it once and checking the reproduction paper for impressions. Machines will be turned off on weekends and holidays.
 - c. The shredder is cleared and the shredder receptacle checked to ensure that the residue is from more than ten shredded pages.
 - d. The telecopier is cleared.

Figure 13-2.--Sample Procedures for Security Checks.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

- e. Security container tops are cleared.
 - f. Individual office spaces are cleared.
 - g. Desk tops are cleared.
 - h. Typewriter ribbons are removed from machines using carbon ribbons on which classified information has been typed.
 - i. Any electrical appliances are disconnected.
 - j. The general area is surveyed and anyone still working with an opened security container will be listed (by name) as an exception next to the item on the security checklist. That person will be responsible for locking and double checking the security container and initialing the checklist showing the time of lockup. Employees will not work alone where Top Secret material is in use or stored or accessible by any one.
3. Each individual is responsible for performing the security check assigned. It is the individual's responsibility to arrange with the Security Manager for a substitute to perform the double check when absence is anticipated. In the unplanned absence of the assigned double checker, the Security Manager will designate a substitute.

Figure 13-2.--Sample Procedures for Security Checks..
Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 14

STORAGE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	14000	14-3
STORAGE REQUIREMENTS.	14001	14-3
SECURITY CONTAINERS	14002	14-3
VAULTS AND STRONGROOMS.	14003	14-4
COMBINATION LOCKS AND COMBINATIONS.	14004	14-4
KEY CONTROL	14005	14-5
ELECTRICALLY ACTUATED LOCKS	14006	14-5
SECURITY CONTAINER DOCUMENTATION.	14007	14-5
SECURING SECURITY CONTAINERS.	14008	14-6
REPAIRING SECURITY CONTAINERS	14009	14-6
INTRUSION DETECTION SYSTEMS (ALARMS).	14010	14-6

FIGURE

14-1	COMBINATION CHANGE ENVELOPE.	14-7
14-2	CLASSIFIED CONTAINER INFORMATION	14-8
14-3	CLASSIFIED CONTAINER CHECK-OUT SHEET	14-9
14-4	PROCEDURES FOR SECURING SECURITY CONTAINERS	14-10

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 14

STORAGE

14000. BASIC POLICY

1. Division and separate branch heads are responsible for safeguarding all classified information under their cognizance. This includes ensuring that it is stored in the manner prescribed in this chapter when it is not being used or is not under the personal observation of cleared persons.
2. Report any weakness or deficiency in equipment used to safeguard classified material in storage to the Security Manager.
3. Do not store valuables, such as money, jewels, precious metals, narcotics, etc., in the same containers used to safeguard classified material. They increase the risk of a container being opened or stolen, with the resulting compromise of the information in it.
4. For identification purposes in the event of emergency destruction or evacuation, place a number or symbol indicating relative priority on the exterior of each security container (i.e., A or I equals Priority I, B or II equals Priority II, and C or III equals Priority III). The external markings will not indicate the level of classified information stored in the container.

14001. STORAGE REQUIREMENTS. All classified material will be secured in a General Services Administration (GSA) approved security container or a certified vault or strongroom. Open storage of classified material is not permitted unless the Security Manager has specifically authorized such storage in writing. Top Secret material will be stored in such a manner as to preclude lone access to that material. Top Secret material will not be openly stored in strongrooms.

14002. SECURITY CONTAINERS. Security containers will not be requested or procured until a requirement has been validated and approved by the Security Manager. All requests for security equipment such as alarms, shredders, security containers and locking devices will be processed via the Security Manager. The Security Manager will maintain security container records forms (OPNAV Form 5510/21) for all security containers. New security equipment will not be placed into service until it has been inspected by CI personnel.

14003. VAULTS AND STRONGROOMS. Certain divisions and separate branches have certified vaults and strongrooms. Open storage in a strongroom after completion of a CI physical security evaluation must be approved in writing by the Security Manager. All work requests for the construction of vaults and strongrooms will be coordinated with the Security Manager and the information provided to the Facilities Officer, Camp H. M. Smith for review. The work request will then be forwarded to the Facilities Office, MCBH.

14004. COMBINATION LOCKS AND COMBINATIONS

1. Only certified combination locks will be used in conjunction with the securing of classified material. The Security Manager maintains a list of approved combination locks which may be used.

2. Combinations will only be changed by trained personnel. A lockout, as a result of an untrained individual attempting to change a combination, could result in administrative action. Combination changes and other container maintenance will be accomplished by providing a DD Form 1149 (Open Purchase Request) to HQSVCBn Supply who will in turn contract the work out to a commercial vendor. CI personnel are available to train SCP personnel in the proper procedures for changing combinations and to perform limited maintenance on an emergency basis only.

3. To help ensure the effectiveness of combination locks, the following requirements apply:

a. Allow only individuals cleared for the highest level of classified material in the container to change combinations.

b. Give the combination only to those whose official duties demand access to the container.

c. Change combinations when placed in use, at least annually thereafter, and when any of the following occurs:

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

(2) The combination has been compromised or the security container has been discovered unlocked and unattended.

(3) The container (with built-in lock) or the padlock is taken out of service. Reset built-in combination locks to the standard combination 50-0. Reset combination padlocks to the standard combination 25-0.

d. In selecting combination numbers, do not use multiples of 5, simple ascending or descending arithmetical series or personal data such as birth dates and serial numbers.

e. Do not use the same combination for more than one container in any one section.

f. In setting a combination, use numbers that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

g. To prevent a lockout, have two different people try a new combination before closing the container or vault door.

h. Assign to the combination of a vault or container, a security classification equal to the highest category of the classified material authorized to be stored in it.

i. Seal records of combinations in an envelope (OPNAV Form 5511/2, figure 14-1). The envelopes containing TOP SECRET and SECRET combinations to the master container, will be stored in the FCC after the appropriate control procedures have been implemented by the CMCC. The recording of combinations will be done immediately after the combinations have been changed.

14005. KEY CONTROL. Division and branch heads will ensure that keys to all offices are maintained within the FCC. This may be a master key to a key box in a central location within the division or branch.

14006. ELECTRICALLY ACTUATED LOCKS. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford the degree of protection required for classified information. These locks are used for the sole purpose of limiting access to a specific area and are not authorized to be used to safeguard classified material.

14007. SECURITY CONTAINER DOCUMENTATION. All security containers, vaults and strongrooms will have the following documentation attached in a conspicuous manner.

1. OPEN and CLOSED sign.

2. Classified Control Information Form (OPNAV 5511/30) showing the names of all persons having knowledge of the combinations. Figure 14-2 indicates the proper method of completing this form.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

3. Classified Container Check-Out Sheet (figure 14-3). These forms are available from HQSVCBN Reproduction.
4. Procedures for Securing the Security Container Form (figure 14-4). These forms are available from the Security Manager.

14008. SECURING SECURITY CONTAINERS. Rotate the dial of combination locks at least four complete turns in the same direction when securing safes, files or cabinets. In most locks, if the dials are given only a quick twist, it is possible to open the lock merely by turning the dial back in the opposite direction. Make sure all drawers of safes and file cabinets are held firmly in the locked position when the equipment has been secured.

14009. REPAIRING SECURITY CONTAINERS. All repairs of security containers will be performed by the facilities office after the submission of a routine work request. CI personnel can provide limited assistance in emergency situations. If containers have been drilled or forced open and repaired, they will not be used for storing classified material until inspected by CI personnel.

14010. INTRUSION DETECTION SYSTEMS (ALARMS). Certain offices incorporate intrusion detection systems as an integral part of the overall physical security deterrent provided to protect classified material. Intrusion detection systems provide a means of detecting and announcing an intrusion which may endanger the security of the space where installed. It must be emphasized that intrusion detection systems are designed to detect, not prevent an attempted intrusion. The PMO reactionary force normally responds to all alarm activations and notifies the respective personnel listed on the alarmed area notification roster. An individual from the section must then respond to all alarm activations. Sections that employ intrusion detection systems will conduct reactionary drills on a quarterly basis. The drill will be a no-notice drill and will be conducted between the hours of 1800 and 0530. The Security Manager will be notified in writing concerning reactionary drills.

**SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM**

WARNING
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS
ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH
APPROPRIATE SECURITY REQUIREMENTS.

SECURITY CONTAINER INFORMATION INSTRUCTIONS		1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).		4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.		6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.		9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		
4. DETACH PART 2A AND INSERT IN ENVELOPE.		10. Immediately notify one of the following persons, if this container is found open and unattended.		
5. SEE PRIVACY ACT STATEMENT ON REVERSE.		EMPLOYEE NAME		
		HOME ADDRESS		
		HOME PHONE		

1. ATTACH TO INSIDE OF CONTAINER 700-101 **STANDARD FORM 700 (8-85)**
NSN 7540-01-214-9372 Prescribed by GSA/1500
32 CFR 2003

CONTAINER NUMBER _____

COMBINATION

_____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____

DETACH HERE

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN
COMBINATION IS ENTERED.
UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN SF 700 (8-85)
ENVELOPE Prescribed by
GSA/1500
32 CFR 2003

Figure 14-1.--Combination Change Envelope.

**SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM**

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PRIVACY ACT STATEMENT ON REVERSE.	1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
	4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
	6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
	9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		
	10. Immediately notify one of the following persons, if this container is found open and unattended.		
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE	

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (6-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 14-2.--Classified Container Information.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

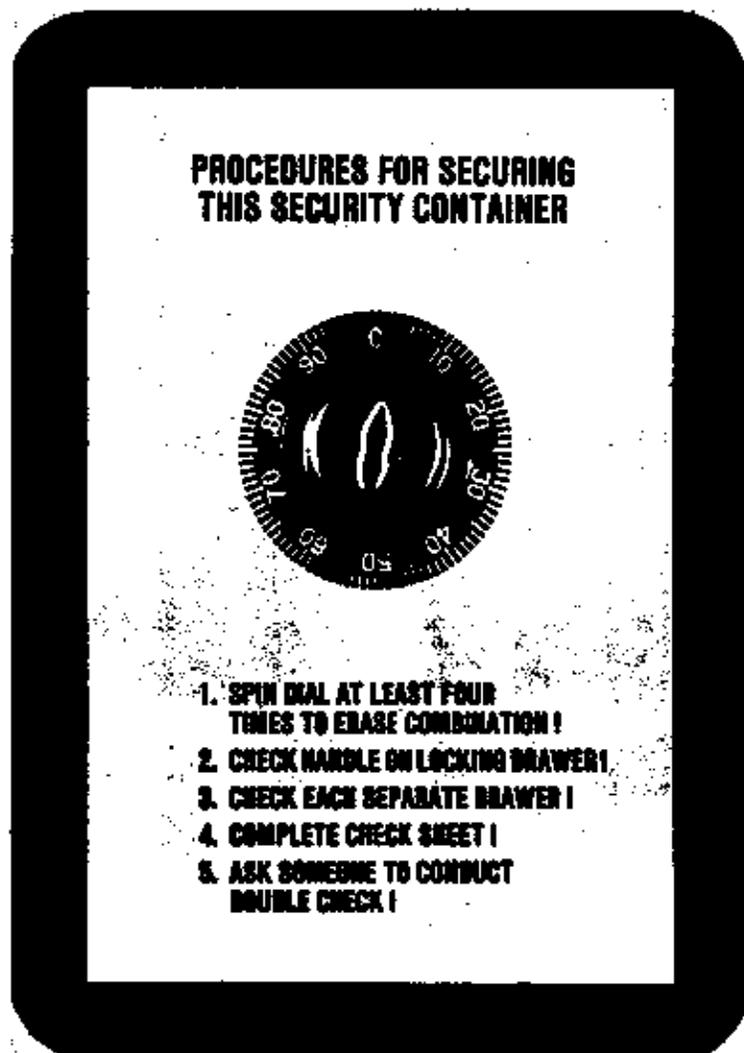


Figure 14-4.--Procedures for Securing Security Containers

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 15

TRANSMISSION OF CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	15000	15-3
TRANSMISSION OF CLASSIFIED MATERIALS FROM THIS HEADQUARTERS	15001	15-3
TELEPHONE TRANSMISSION.	15002	15-4
RECEIPT SYSTEM.	15003	15-4
TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS	15004	15-4
TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL.	15005	15-4
PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION	15006	15-4
ADDRESSING.	15007	15-4

FIGURE

15-1	RECORD OF RECEIPT	15-5
------	-----------------------------	------

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 15

TRANSMISSION OF CLASSIFIED MATERIAL

15000. BASIC POLICY

1. Classified information will be transmitted either in the custody of an appropriately cleared individual, by an approved system or carrier and per the provisions of this chapter.
2. The term transmission refers to any movement of classified information or material from one place to another.
3. The carrying of classified material across national borders is not permitted unless arrangements have been made that will preclude customs, postal or other inspections. In addition, foreign carriers may not be used unless the U.S. escort has physical control of the classified material at all times.

15001. TRANSMISSION OF CLASSIFIED MATERIALS FROM THIS HEADQUARTERS. All classified materials to be transmitted from this headquarters will be processed through the appropriate control points.

1. CMCC. All Top Secret (including SPECAT messages), Secret, and Confidential documents will be processed through the CMCC prior to transmission. This includes documents to be transferred to other commands on the island for retention by those commands. Divisions and separate branches are prohibited from mailing any classified material from this headquarters, with the exception of the AC/S G-2, who transmits special access materials.
2. FCC. Certain classified materials may be processed and transmitted over the approved secure telecopier and facsimile circuits. Top Secret material will not be processed over these circuits without first processing it through the TSCO and the CMCC for appropriate controls.
3. SIH. Divisions and separate branches are authorized to transmit Secret and Confidential messages through the SIH. All Top Secret messages will be processed through the TSCO and the CMCC for appropriate controls.
4. SSO. All SCI materials transmitted will be processed through the SSO.

15002. TELEPHONE TRANSMISSION

1. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits.
2. This headquarters does have approved secure telephone circuits which can be used for all calls involving classified information.
3. The FCC has an approved secure telecopier capability to other major commands within the Marine Corps.
4. All nonsecured telecopiers will display the following warning notice: "THIS EQUIPMENT IS NOT AUTHORIZED FOR THE TRANSMISSION OF CLASSIFIED INFORMATION."

15003. RECEIPT SYSTEM. All Top Secret, Secret, and Confidential material (except messages) prepared and transmitted from this headquarters will be accompanied by a receipt for the material. Receipts will be retained for at least two years. A sample receipt form is attached as figure 15-1.

15004. TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS. Personnel are prohibited from releasing classified material or information to representatives of foreign governments without the approval of the Security Manager.

15005. TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL. COMSEC material will only be transmitted by the CMS custodian or in the case of "over-the-air re-keying (OTAR)", only by trained and cleared circuit operators.

15006. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION. All classified documents transmitted will be prepared for shipment by the CMCC.

15007. ADDRESSING. Classified material will only be addressed to an official government activity or DoD contractor and not an individual. Office codes and such phrases as "Attention LtCol ALLEN" are permitted on inner envelopes to expedite internal routing.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

RECORD OF RECEIPT
(REFERENCE SECURITYINST 3514.9)

THIS RECEIPT MUST BE
SHOWED AND RETURNED.

OPNAV 551/19 (REV. 4-79)
N7N 000-LP-088-1131

ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF MATERIAL	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF ENCL. TO MATL RCD	REGISTERED NUMBER

ADDRESS (ACTIVITY RECEIVING MATERIAL)

SIGNATURE (Authorized Receipt)

DATE

U.S. GOVERNMENT PRINTING OFFICE: 1985-507-239

Figure 15-1.--Record of Receipt.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

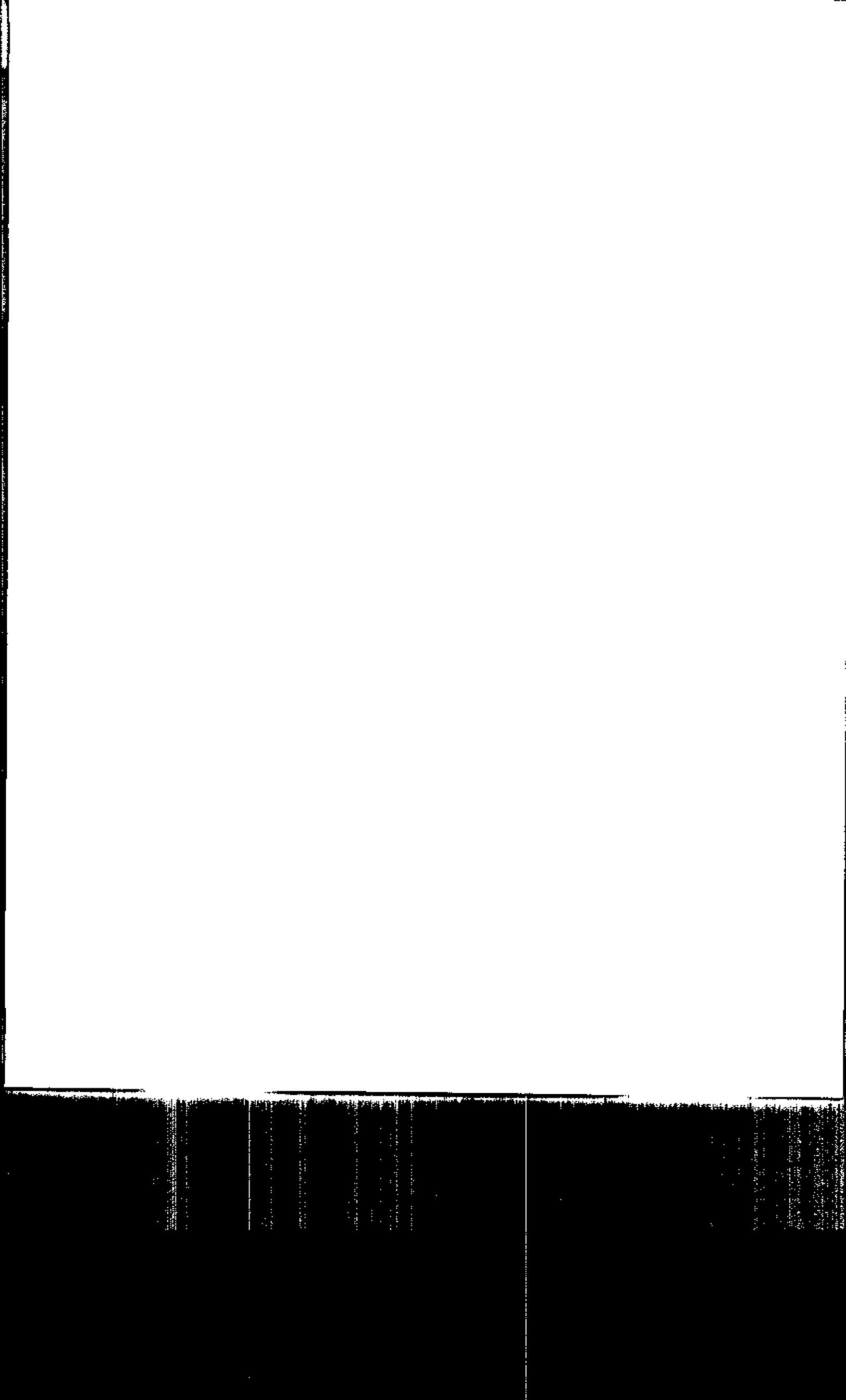
CHAPTER 16

HANDCARRYING CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	16000	16-3
HANDCARRYING WITHIN CAMP H. M. SMITH INSTALLATION.	16001	16-3
HANDCARRYING AROUND OAHU.	16002	16-3
AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS	16003	16-3
PROTECTION OF CLASSIFIED MATERIAL WHILE HANDCARRYING IN A TRAVEL STATUS . . .	16004	16-4
HANDCARRYING CLASSIFIED MATERIAL ON COMMERCIAL PASSENGER AIRCRAFT.	16005	16-5
PROCEDURES FOR CARRYING CLASSIFIED DOCUMENTS ABOARD COMMERCIAL PASSENGER AIRCRAFT.	16006	16-6
HANDCARRYING CLASSIFIED MATERIAL IN PACKAGES ABOARD COMMERCIAL PASSENGER AIRCRAFT.	16007	16-6
DOCUMENTATION REQUIRED TO CARRY CLASSIFIED MATERIAL ABOARD COMMERCIAL PASSENGER AIRCRAFT	16008	16-6
CONDUCT OF PASSENGERS ON HIJACKED AIRCRAFT	16009	16-7

FIGURE

16-1	REQUEST FOR AUTHORIZATION TO HAND CARRY CLASSIFIED MATERIAL ABOARD COMMERCIAL CHARTERED AIRCRAFT.	16-9
16-2	AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL ABOARD COMMERCIAL CHARTERED AIRCRAFT/RETURN ENDORSEMENT.	16-10
		16-1



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 16

HANDCARRYING CLASSIFIED MATERIAL

16000. BASIC POLICY. Every precaution must be taken to prevent unauthorized disclosure when individuals are handcarrying classified material in the pursuit of daily duties or outside this headquarters in a travel status.

16001. HANDCARRYING WITHIN THE CAMP H. M. SMITH INSTALLATION. All classified material handcarried aboard Camp H. M. Smith will be protected in appropriate classified document folders commensurate with the highest classification of the material contained therein. Bulk materials will also be protected with appropriate covers to prevent casual observation by unauthorized individuals. Classified material will not be carried into common areas such as the PX, snack bar, laundry, or barber shop.

16002. HANDCARRYING AROUND OAHU. All classified materials handcarried outside the "confines" of Camp H. M. Smith will be double wrapped and secured in a briefcase. The briefcase may be considered the outer wrapping when transporting classified material on the island. When classified material being carried is actually being transferred to another command for retention, the requirements of chapter 15 of this Manual will be adhered to. An inventory will be maintained by the appropriate division or separate branch of all documents handcarried from this headquarters to other commands on the island. CMCC controlled documents will be routed through the CMCC prior to being removed from this headquarters. The individual directly senior to the person carrying the classified material will personally obtain authorization and ensure the material is transmitted per the instructions of this Manual.

16003. AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS

1. Except under extraordinary or emergency circumstances, individuals from this headquarters will not be authorized to handcarry classified material off the island of Oahu. Handcarrying will be authorized only under the following circumstances:

a. The classified material is required at the traveler's destination.

b. The classified material is not available at the command to

be visited.

c. Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

2. The Security Manager must be advised when anyone in a travel status needs to handcarry classified material to or from this headquarters. The Security Manager can ensure the proper procedures for handcarrying classified material are followed and that the traveler fully understands the responsibility for safeguarding the classified material. Requests to handcarry classified material will be provided to the Security Manager ten (10) working days prior to the departure date of the individual.

3. Failure of an individual, division or branch to transmit required classified materials by approved methods of transmission in a timely manner, is not considered adequate justification to require approval to handcarry the material.

4. When a courier letter is required, the following information will be provided in the form of a request (see figure 16-1 Request for Authorization to Handcarry Classified Material Aboard U.S. Commercial Chartered Aircraft) to the Security Manager:

- a. The full name of the individual traveling.
- b. Social Security Number/MOS.
- c. Courier Card Number and expiration date.
- d. Armed Forces Identification Card Number.
- e. Description of material being carried (e.g., three sealed packages, 9" x 8" x 24") addressee, and sender.
- f. The point of departure, destination, and known transfer points.
- g. Point of Contact and telephone number where material will be stored.
- h. Inclusive dates of travel.

16004. PROTECTION OF CLASSIFIED MATERIAL WHILE HANDCARRYING IN A TRAVEL STATUS. Prior to handcarrying classified material, individuals will become familiar with the following:

1. The classified material must be in an individual's physical possession at all times, unless proper storage at a U.S.

Government activity or appropriately cleared contractor facility (continental U.S. only) is available. Handcarrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage in a government activity or a cleared facility. The Security Manager must approve the use of such a facility prior to the individual conducting the travel. When surrendering any package containing classified material for temporary storage (e.g., overnight or during meals), an individual must obtain a receipt signed by an authorized representative of the contractor facility or government installation accepting responsibility for safeguarding the package.

2. Classified material may not be read, studied, displayed, or used in any manner on a public conveyance or in a public place.

3. When classified material is carried in a private, public or government conveyance, it will not be stored in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank.

4. A list of all classified material carried or escorted will be maintained by the CMCC and must be accounted for upon return.

5. Unless unusual circumstances exist, all handcarried classified material will be returned to this headquarters by one of the approved methods of transmission.

16005. HANDCARRYING CLASSIFIED MATERIAL ON COMMERCIAL PASSENGER AIRCRAFT

1. Classified material will only be transported aboard commercial passenger aircraft when other methods will not transmit the material in time to meet operational requirements. Lack of prior planning which results in insufficient time to transmit the material, usually will not be sufficient justification to handcarry the material.

2. The AC/S G-1 in the name of the Commander, is the authorizing official who may approve the handcarrying of classified material aboard commercial passenger aircraft. Each individual transmitting classified material must obtain this authorization (figure 16-2 refers) in writing.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM16006. PROCEDURES FOR CARRYING CLASSIFIED DOCUMENTS ABOARD
COMMERCIAL PASSENGER AIRCRAFT

1. A traveler carrying classified documents aboard a commercial aircraft will process through the airline ticketing and boarding procedures in the same manner as all other passengers.
2. Travelers will ensure the following:
 - a. They have the required documentation described in paragraph 16008 of this Manual.
 - b. Make sure the classified documents being carried have no metal bindings and are in double sealed envelopes. All documents will be double wrapped with an inner and outer envelope and be contained in a locked briefcase.
 - c. Present yourself at the screening station for routine processing. If you are carrying the documents in a briefcase or other carry-on luggage, the briefcase or luggage will be routinely offered for opening for inspection. The screening official will then be able to inspect the envelopes by flexing, feel, weight, etc., without any requirement for opening the envelopes themselves.
 - d. If the screening official is not satisfied, you will inform the official that the envelopes contain classified material and you will then exhibit an official U.S. Government identification card, plus your travel authorization. At that point, the screening official will process the envelopes with a detection device. If no alarm results, the envelopes require no further examination. But, if an alarm sounds, you will not be permitted to board and therefore, will not be subject to further screening for boarding purposes. Opening or reading the classified documents by the screening official is never permitted. If the official insists, advise the Security Manager immediately.

16007. HANDCARRYING CLASSIFIED MATERIAL IN PACKAGES ABOARD
COMMERCIAL PASSENGER AIRCRAFT. Normally, individuals from this headquarters will not be authorized to handcarry large enough quantities of classified material to require packaging such materials. The Security Manager will be advised if such a requirement exists.

16008. DOCUMENTATION REQUIRED TO CARRY CLASSIFIED MATERIAL ABOARD
COMMERCIAL PASSENGER AIRCRAFT

1. When carrying classified material, as described in paragraph 16006 above, the traveler must have a picture identification card

and travel authorization which specifically describes the envelopes containing the classified material and the DD Form 2501, Courier Authorization Card.

2. The traveler will also carry the original of the letter of authorization to handcarry classified material. A reproduced copy is not acceptable; however, travelers should have sufficient authenticated copies to provide a copy to each airline involved. The letter will be prepared on letterhead stationery of this headquarters by the Security Manager or the designated representative.

16009. CONDUCT OF PASSENGERS ON HIJACKED AIRCRAFT

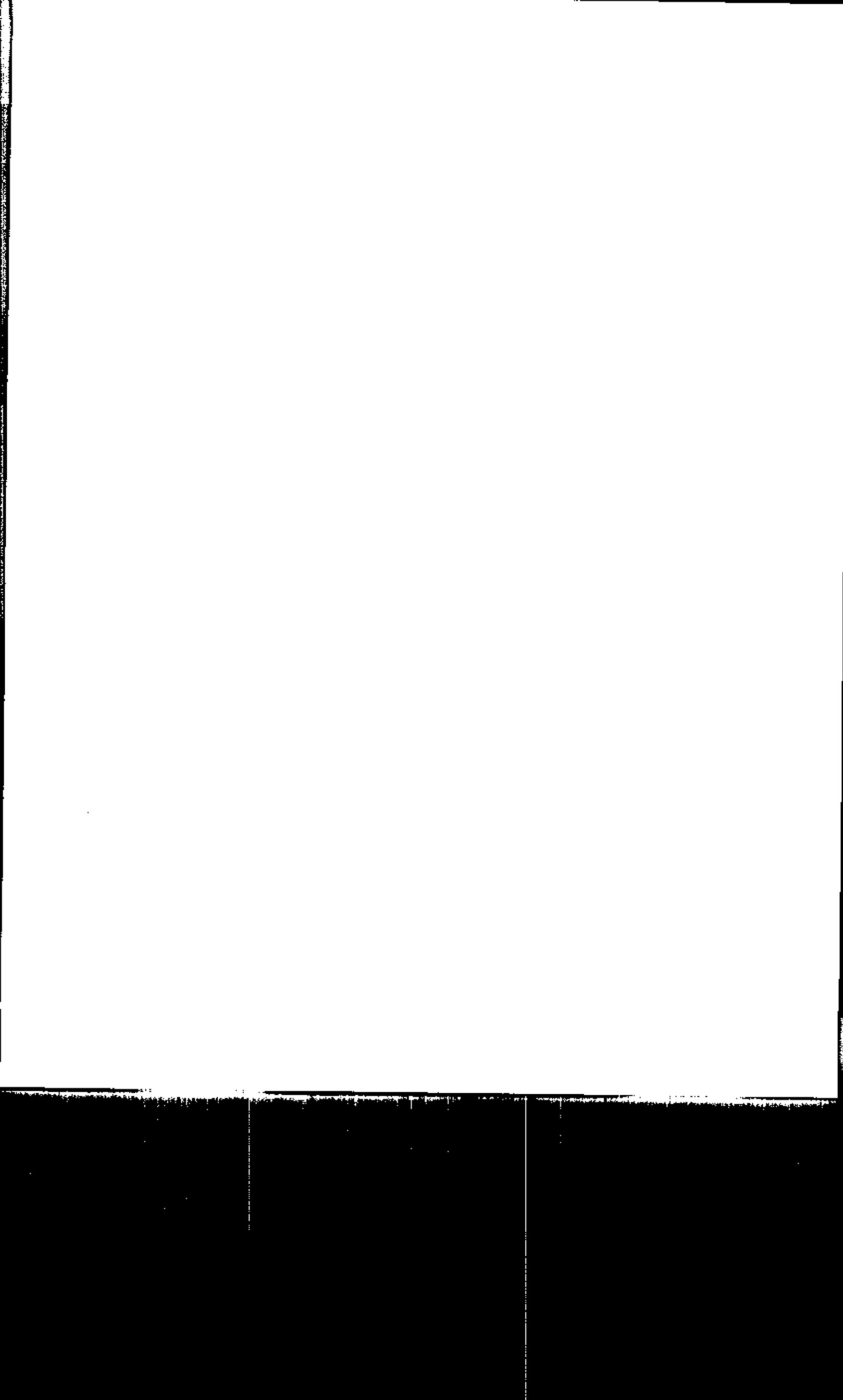
1. Personnel handcarrying classified material on commercial passenger aircraft will be aware of the following guidance for their conduct if the plane is hijacked and made to land in a foreign country:

a. If identification is required and you are in uniform, show your Armed Forces or civilian identification card. If you are in civilian clothes, show civilian identification initially; however, if you are asked directly if you are in the Armed Forces, you should not attempt to deny your military affiliation.

b. If you are questioned in a foreign country, use common sense in making any response, but do not under any circumstances reveal classified information.

c. Upon your return to U.S. control, official U.S. investigators may want to debrief you. You should, therefore, observe and mentally note the methods and procedures used by the detainers during your stay in their country.

2. If, as a result of hijacking of an aircraft to a foreign country classified material is compromised or subjected to compromise, or there are indications of foreign intelligence exploitation of personnel or material, notify the Security Manager immediately.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5510
2E

From: (Requesting Division/Section/Activity)
To: Security Manager

Subj: **REQUEST FOR AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL
ABOARD COMMERCIAL CHARTERED AIRCRAFT**

Ref: (a) OPNAVINST 5510.1H
(b) MARFORPACO 5510.18

1. Per the references, request authorization to handcarry classified material up to and including SECRET, aboard commercial aircraft in the performance of assigned duties.
2. Storage arrangements per the references have been made with the CINCCENT CMCC. POC is 1stLt N. F. Storer, phone AV XXX-XXXX.
3. The following information is provided:
 - a. Full Name: Joseph A. Giardino
 - b. Grade: Master Sergeant
 - c. U.S. Courier Card Number: #AS 00000 Expires: 950505
 - d. Military Identification Card Number: N1234567880
 - e. Itinerary: Depart Honolulu, HI 8 Jan 95
Arrive Tampa, Florida 9 Jan 95
Return Honolulu, HI 12 Jan 95
 - f. Date Courier Authorization Issued: 6 Jan 95
 - g. Date Courier Authorization Expires: 13 Jan 95
 - h. Description of Material: Two manila envelopes
4. POC: LtCol I. A. / Johnson, Deputy, 477-XXXX

I. M. JOHNSON

Figure 16-1.--Request for Authorization to Handcarry
Classified Material Aboard Commercial
Chartered Aircraft.

16-9

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5510
01

From: Assistant Chief of Staff, G-1 (Security Manager)
To: Master Sergeant Joseph A. Giardino XXX XX XXXX
Subj: AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL ABOARD
COMMERCIAL CHARTERED AIRCRAFT
Ref: (a) OPNAVINST 5510.1H
Encl: (1) (Label paragraphs)
(2) (Certification of paragraphs)

1. Per the reference, you are authorized to handcarry classified material, up to and including SECRET, aboard commercial aircraft in the performance of your assigned duties. You are directed to read paragraphs 15-2 (subparagraphs 1-9) and 16-3 through 16-7 provided as enclosure (1).
2. Prior to your departure, you will ensure that the classified material is checked out via the MARFORPAC CMCC for proper packing. Additionally, you will ensure that appropriate storage arrangements have been made at your point of destination.
3. Enclosure (2) will be completed and returned to the Security Manager prior to your departure acknowledging that you have properly completed all provisions of enclosure (1).
4. COMMARFORPAC POC for telephone verification is Major Edward R. Dunlap, Assistant Security Manager, Commercial: (808)/DSN (315) 477 XXXX/XXXX. After normal working hours contact the FCC at Commercial (808)/DSN: (315) 477-0077 (24 hours).

E. R. SECURITY
By direction

Figure 16-2.--Authorization to Handcarry
Classified Material Aboard
Commercial Chartered Aircraft.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5510
(Date)

(RETURN ENDORSEMENT)

From: Master Sergeant J. A. Giardino XXX XX XXXX
To: Assistant Security Manager

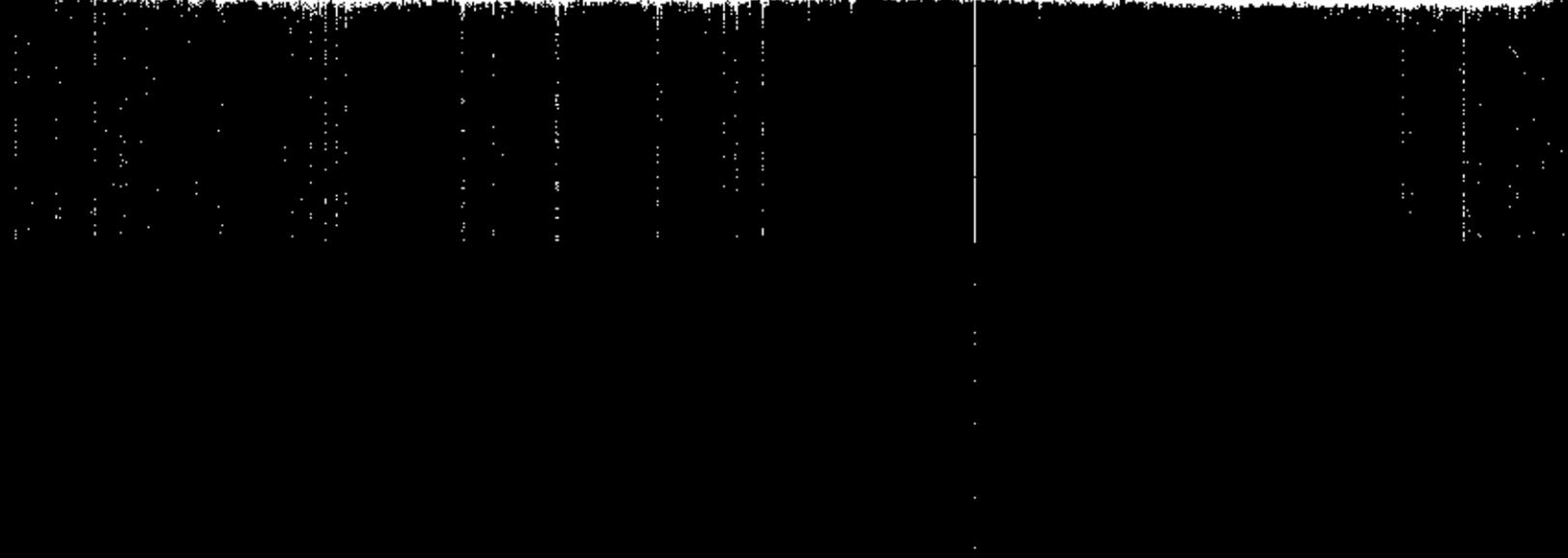
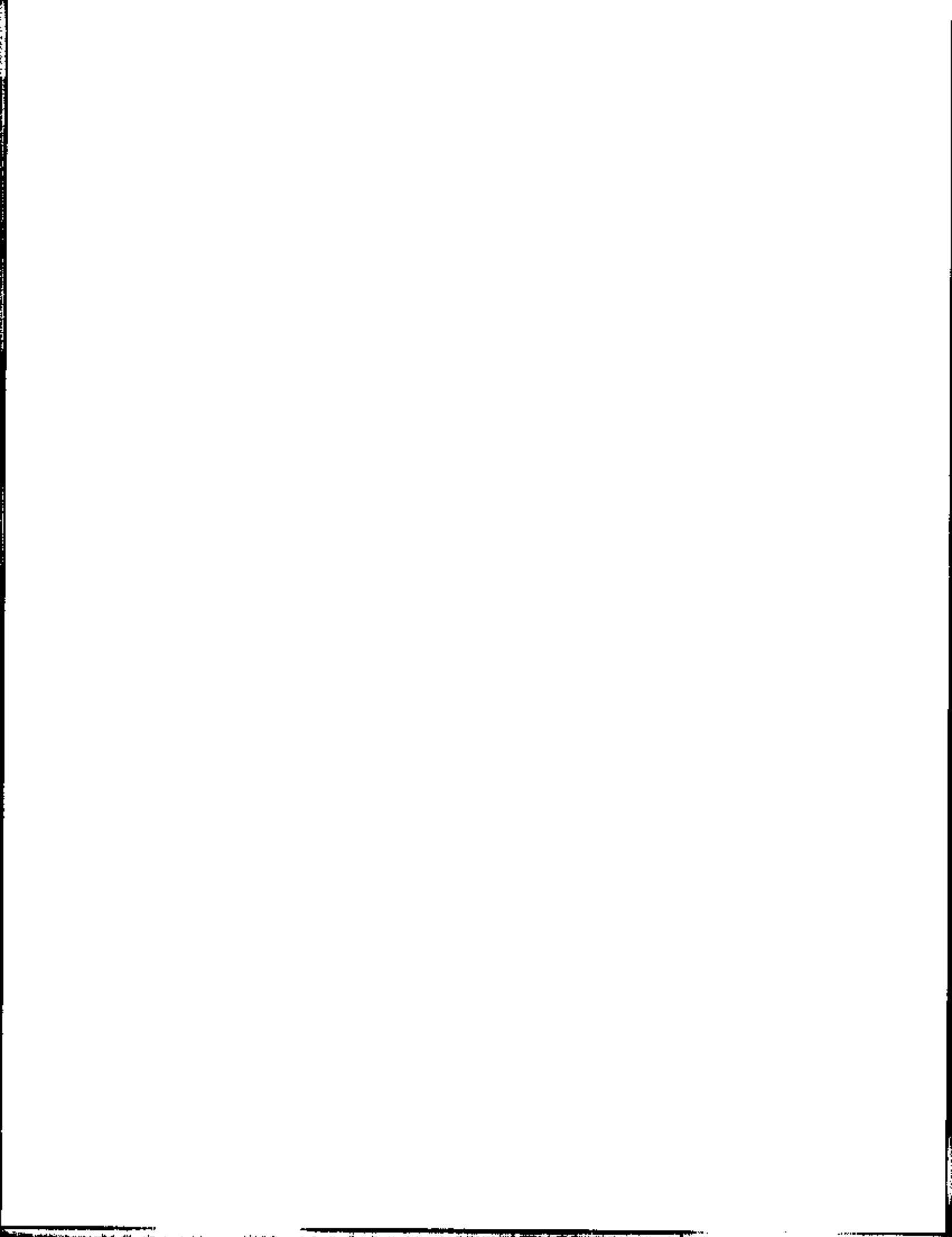
Subj: COMPLETION OF REQUIREMENTS LISTED IN PARAGRAPHS ONE, TWO
AND THREE OF BASIC CORRESPONDENCE

1. Acknowledge completion of requirements identified in the basic correspondence.
2. Acknowledge that a receipt will be obtained for any classified material released to the commands visited.

J. A. GIARDINO

Figure 16-2.--Authorization To Handcarry
Classified Material Aboard
Commercial Chartered Aircraft--
Return Endorsement

16-11



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

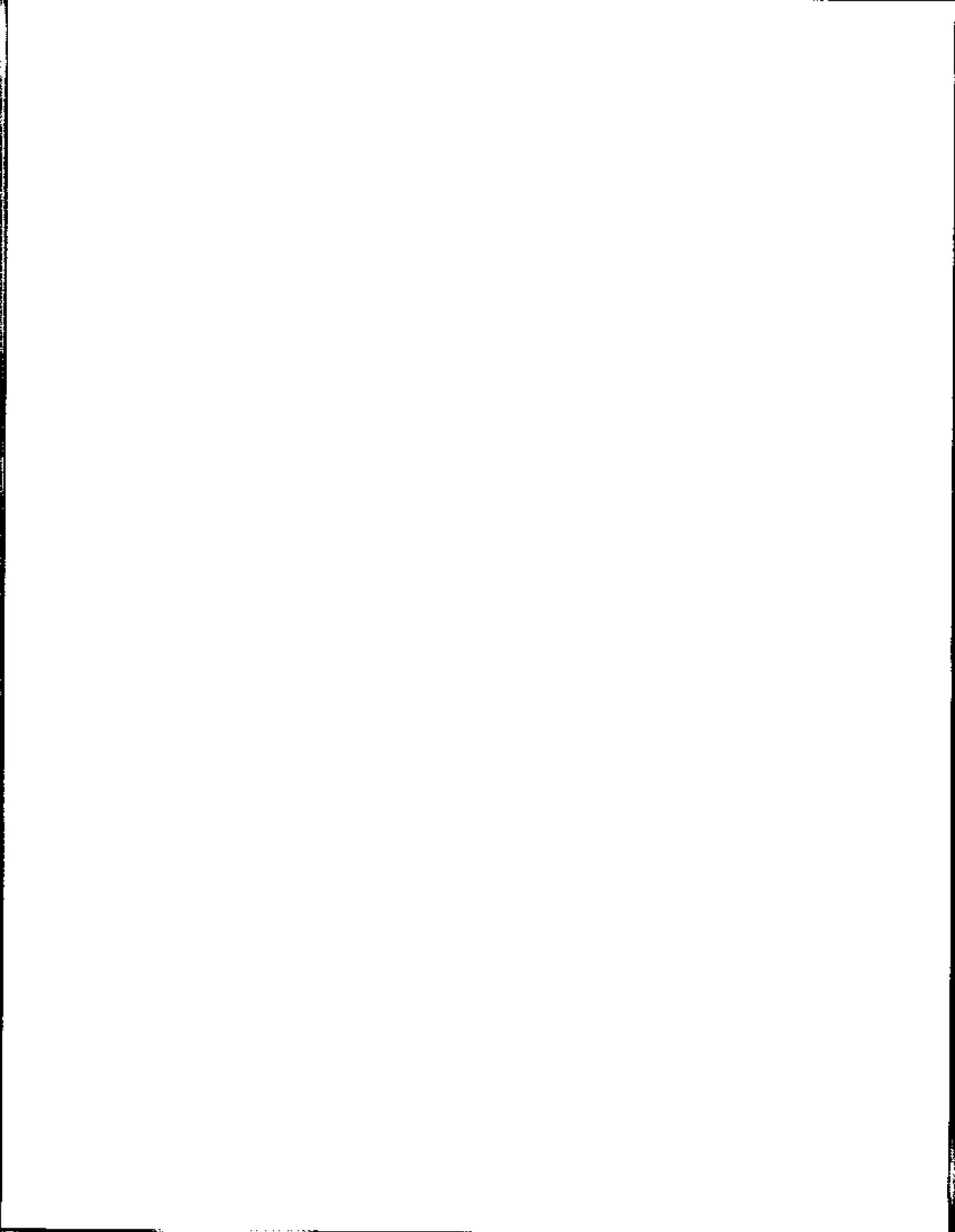
CHAPTER 17

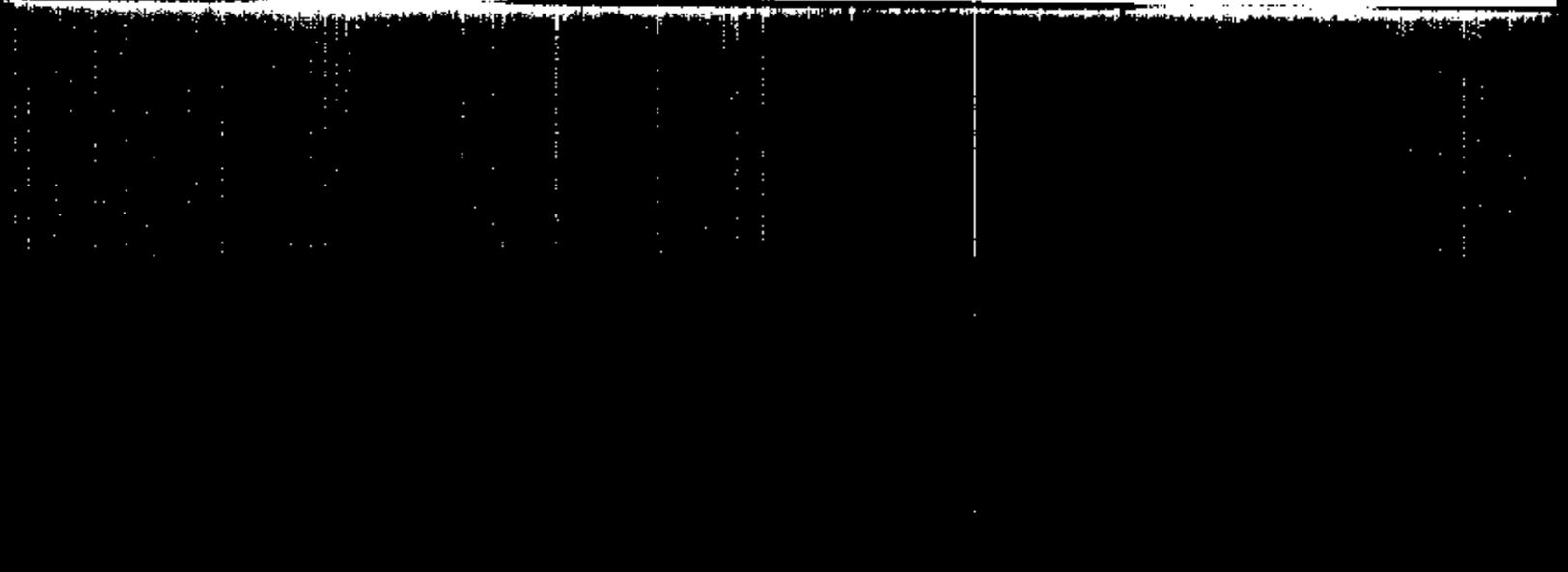
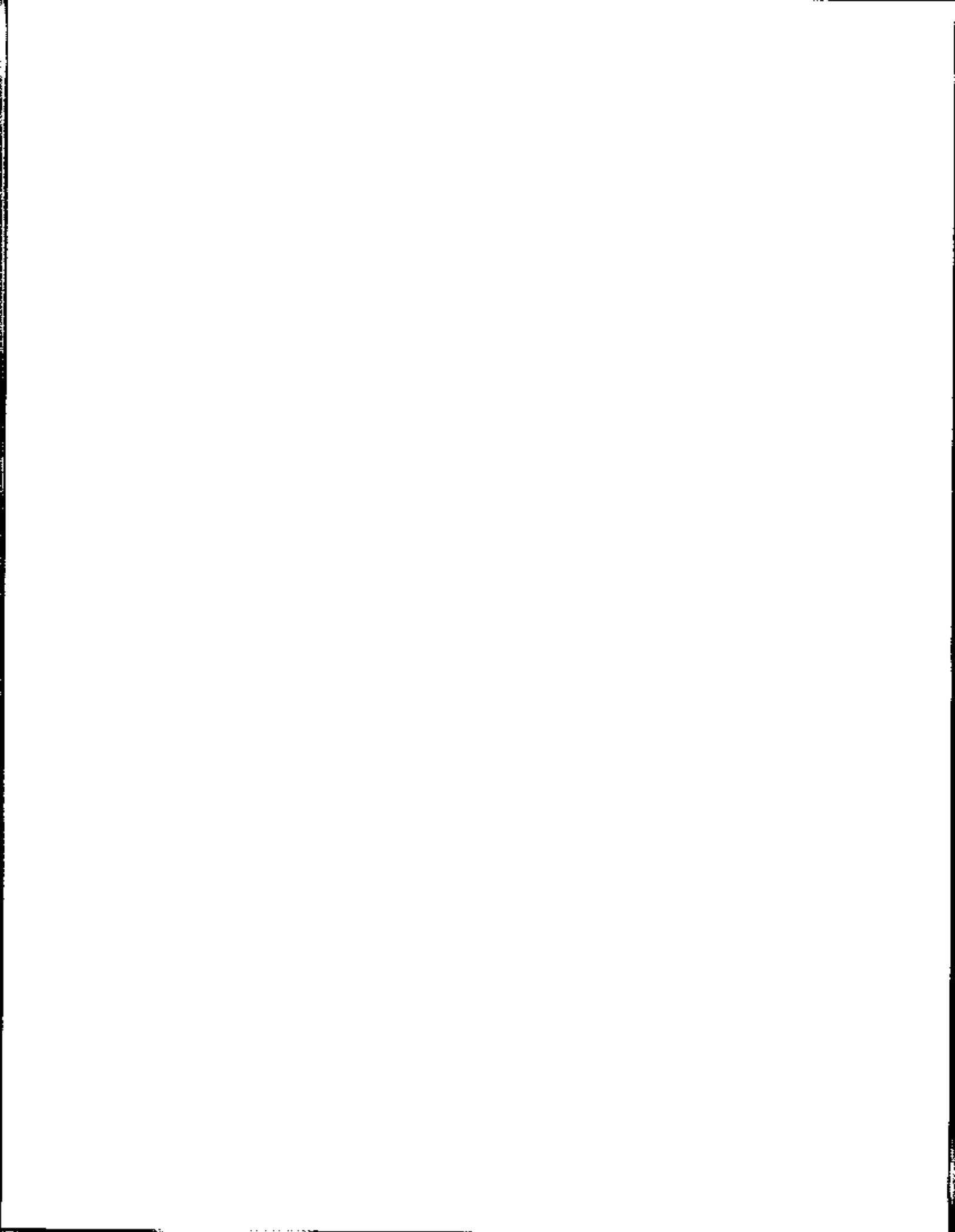
DESTRUCTION OF CLASSIFIED MATERIAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	17000	17-3
DESTRUCTION PROCEDURES.	17001	17-3
METHODS OF DESTRUCTION.	17002	17-4
DECLASSIFYING OR CLEARING ADP MEDIA	17003	17-5
DESTRUCTION OF UNCLASSIFIED MATERIAL.	17004	17-5
EMERGENCY DESTRUCTION	17005	17-5
PRIORITY FOR EMERGENCY DESTRUCTION.	17006	17-7

FIGURE

17-1	FORMAT FOR CERTIFICATE OF DECLASSIFICATION OF CLASSIFIED MAGNETIC TAPES.	17-9
------	--	------





SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 17

DESTRUCTION OF CLASSIFIED MATERIAL

17000. BASIC POLICY

1. Classified record material may be destroyed only when destruction is the disposition authorized by the current edition of SECNAVINST 5212.5, Disposal of Navy and Marine Corps Records.
2. All other classified material will be destroyed as soon as it is no longer required. Early disposal of unnecessary classified material can assist in reducing security costs, preparing for emergency situations and better protecting necessary classified material. Classified material over five years old will not be retained without proper justification being provided to the Security Manager.
3. Destruction of CMS materials will be accomplished only by the CMS custodian or alternate custodian.

17001. DESTRUCTION PROCEDURES

1. Classified material will only be destroyed by authorized means and by personnel cleared to the level of the material being destroyed.
2. Classified material awaiting destruction will be afforded the protection equal to the highest classification of information it contains. Safeguard "burn bags" at the level of the highest classification they contain until they are completely destroyed.
3. The CMCC is responsible for the destruction of all accountable documents entered into this headquarters' classified accountability system. Documents awaiting destruction will be returned to CMCC.
4. The CMCC will record the destruction of all Top Secret and Secret material (with the exception of Secret messages). These records will be maintained for two years.
5. Two officials will be present for the destruction of all classified material destroyed within this headquarters. One official will destroy the material and the other will witness the destruction. At least one of the individuals will be an E-5 or above.
6. Confidential material and classified waste (Secret and Confidential) may be destroyed without a record of destruction.

This headquarters has a waiver on the requirement to record the destruction of Secret messages; however, the requirement still exists for two officials to accomplish the destruction as identified in paragraph 17001.5 above.

7. The CMCC will post the security responsibilities of the users of the destruction equipment and must assume any unassigned responsibilities. The CMCC will ensure that destruction is complete and that reconstruction of classified material is impossible.

17002. METHODS OF DESTRUCTION

1. The CMCC operates an approved disintegrator for most classified materials which need to be destroyed. Arrangements will be made with CMCC to schedule an appointment to use the equipment. Divisions and separate branches will provide their own personnel to accomplish the destruction of messages and classified waste. The CMCC will post the proper procedures for operating the CMCC disintegrator. These procedures will be adhered to by all individuals using the equipment.
2. Certain divisions and separate branches have approved shredders which may be used for the destruction of classified materials. The Security Manager will certify all destruction equipment prior to use for classified material. Open purchase requests (DD Form 1199) to purchase shredders or other destruction equipment will be provided to supply via the Security Manager to ensure the equipment meets the criteria for destroying classified material.
3. Shredders are not authorized for use in destroying classified microfiche. All shredders will permanently display the following warning notice; "THIS MACHINE IS NOT AUTHORIZED FOR THE DESTRUCTION OF CLASSIFIED MICROFICHE."
4. Under certain circumstances, the shredder within CMCC may not be operational. During these periods, CMCC will arrange for an alternate means of destroying classified materials.
5. Another destruction facility is located at U.S. Naval Base, Pearl Harbor and will only be used when the primary is out of order or when a sufficient amount of microfiche or microfilm is accumulated to warrant its use. The CMCC will arrange for use of the Pearl Harbor facility.
6. The CMCC has limited storage area for classified (waste) material pending destruction. Accordingly, SCPs must routinely destroy classified waste and not permit an accumulation in excess of SCP storage capabilities. In the event of an unexpected

This headquarters has a waiver on the requirement to record the destruction of Secret messages; however, the requirement still exists for two officials to accomplish the destruction as identified in paragraph 17001.5 above.

7. The CMCC will post the security responsibilities of the users of the destruction equipment and must assume any unassigned responsibilities. The CMCC will ensure that destruction is complete and that reconstruction of classified material is impossible.

17002. METHODS OF DESTRUCTION

1. The CMCC operates an approved disintegrator for most classified materials which need to be destroyed. Arrangements will be made with CMCC to schedule an appointment to use the equipment. Divisions and separate branches will provide their own personnel to accomplish the destruction of messages and classified waste. The CMCC will post the proper procedures for operating the CMCC disintegrator. These procedures will be adhered to by all individuals using the equipment.
2. Certain divisions and separate branches have approved shredders which may be used for the destruction of classified materials. The Security Manager will certify all destruction equipment prior to use for classified material. Open purchase requests (DD Form 1199) to purchase shredders or other destruction equipment will be provided to supply via the Security Manager to ensure the equipment meets the criteria for destroying classified material.
3. Shredders are not authorized for use in destroying classified microfiche. All shredders will permanently display the following warning notice; "THIS MACHINE IS NOT AUTHORIZED FOR THE DESTRUCTION OF CLASSIFIED MICROFICHE."
4. Under certain circumstances, the shredder within CMCC may not be operational. During these periods, CMCC will arrange for an alternate means of destroying classified materials.
5. Another destruction facility is located at U.S. Naval Base, Pearl Harbor and will only be used when the primary is out of order or when a sufficient amount of microfiche or microfilm is accumulated to warrant its use. The CMCC will arrange for use of the Pearl Harbor facility.
6. The CMCC has limited storage area for classified (waste) material pending destruction. Accordingly, SCPs must routinely destroy classified waste and not permit an accumulation in excess of SCP storage capabilities. In the event of an unexpected

overflow, the SCP custodian will contact the OIC CMCC to arrange for temporary stowage.

17003. DECLASSIFYING OR CLEARING ADP MEDIA

1. ISMO has authorized equipment for degaussing magnetic tapes. All requests for such service will be provided to the ADP Security Officer for appropriate action. Upon declassification of magnetic tapes, etc., the tapes will be reviewed for complete degaussing. A letter (see figure 17-1 for format) will be delivered to the Security Manager for review. The Security Manager will endorse the letter indicating that the tapes have to be declassified and are ready for destruction. The HQSVCBn MARFORPAC Supply Officer will then forward the tapes to the Disposal Unit, Pearl Harbor for destruction.

2. All equipment that employs a magnetic media or memory device which is used in the production of classified material, will be inspected by CI personnel prior to being returned to supply or removed from this headquarters by maintenance personnel. When equipment is returned following repair, it will also be checked by CI personnel. Equipment used in the preparation of classified material requiring a TEMPEST inspection will be reinspected each time it has been repaired.

17004. DESTRUCTION OF UNCLASSIFIED MATERIAL

1. The policy within this headquarters is that all messages, regardless of classification, will be destroyed by shredding. There are no exceptions to this requirement.

2. All material bearing the control caveat "FOUO", will be destroyed by tearing each copy into pieces to prevent reconstruction and placing the residue into regular trash receptacles per the current edition of SECNAVINST 5720.42.

3. Technical manuals bearing any limited distribution statements will be handled and destroyed in the same manner as "For Official Use Only" material.

17005. EMERGENCY DESTRUCTION

1. All divisions and separate branches that store classified material will formulate an emergency destruction plan for materials under their cognizance. A copy of the division and separate branch emergency destruction plan will be forwarded to the OIC CMCC.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

2. The OIC CMCC will formulate the overall emergency destruction plan, implementing the input provided by the respective sections. The command emergency destruction plan will:

a. Emphasize the procedures and methods of destruction. Clearly identify the exact location of all classified material. Include priorities for destruction, billet designations of personnel responsible for destruction and the prescribed place and method of destruction. Additionally, if any destruction site or any particular piece of destruction equipment is to be used by more than one activity or entity, clearly delineate the order or priority for use of the site or equipment.

b. Authorize the senior individual present, in an office containing classified material, to deviate from established plans when circumstances warrant.

c. Identify the individual who is authorized to make the determination as to when emergency destruction is to begin and the means by which this determination is to be communicated to all subordinate elements maintaining classified information.

d. Emphasize the importance of beginning destruction early enough to preclude loss of material. The effect of premature destruction is inconsequential when measured against the possibility of compromise under emergency conditions.

5. Any reasonable means to ensure the classified material cannot be reconstructed, should be approved for use in emergency destruction. Ideally, the destruction method will provide for early attainment of a point at which the destruction process is irreversible.

6. The equipment used for routine destruction of classified material should perform a major role in the headquarters' plan for emergency destruction.

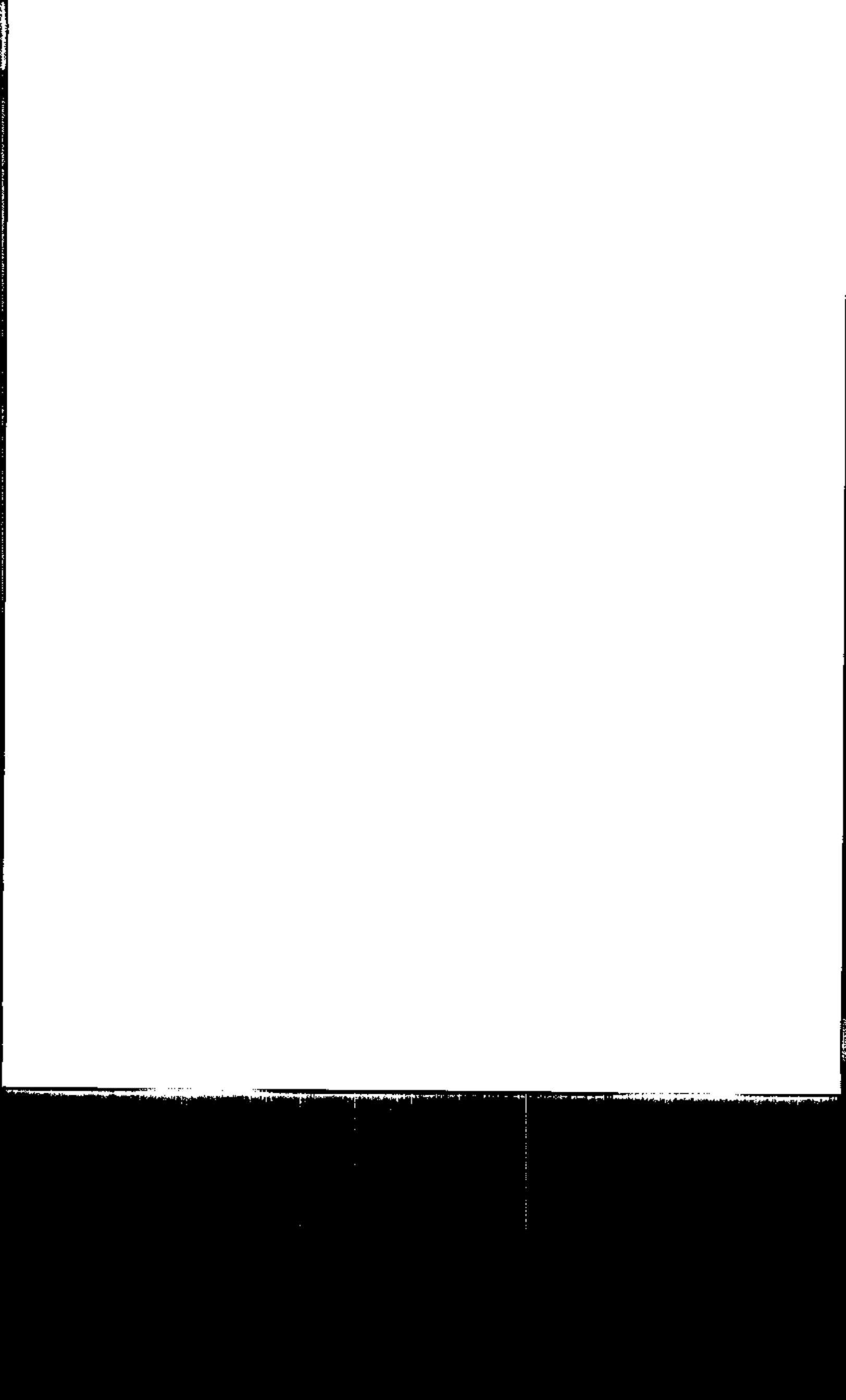
7. Emergency destruction drills will be conducted periodically (at least annually) to ensure that personnel are familiar with the plan and associated equipment. The drills will also be used to evaluate the anticipated effectiveness of the plan and prescribed equipment, and should be the basis for improvements in planning and equipment use.

8. The plan will also identify procedures to be implemented in the case of natural disasters or emergencies such as a fire.

9. The plan will include procedures for reporting emergency destruction in accordance with the current edition of OPNAVINST 5510.1.

17006. PRIORITY FOR EMERGENCY DESTRUCTION

1. In the emergency plan, assign a priority for emergency evacuation and destruction of classified holdings. Priorities will be based on the potential effect on national security should holdings fall into hostile hands.
2. The priorities for emergency destruction are as follows:
 - a. Priority One. Top Secret material/Special Compartmented Information and Special Access materials.
 - b. Priority Two. Secret material.
 - c. Priority Three. Confidential material.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SSIC
Office Code
Date

From: (Responsible Officer)
To: Disposal Unit Officer
Via: (1) Security Manager
(2) Camp Supply Officer, HQSVCBn

Subj: CERTIFICATE OF DECLASSIFICATION OF CLASSIFIED MAGNETIC TAPES

Ref: (a) MARFORPACO P5510.18

Encl: (1) (Description/List of Tapes)

1. Per the reference, I hereby certify that the enclosed tapes were declassified and are ready for destruction.

(Signature)

SSIC
Office Code
Date

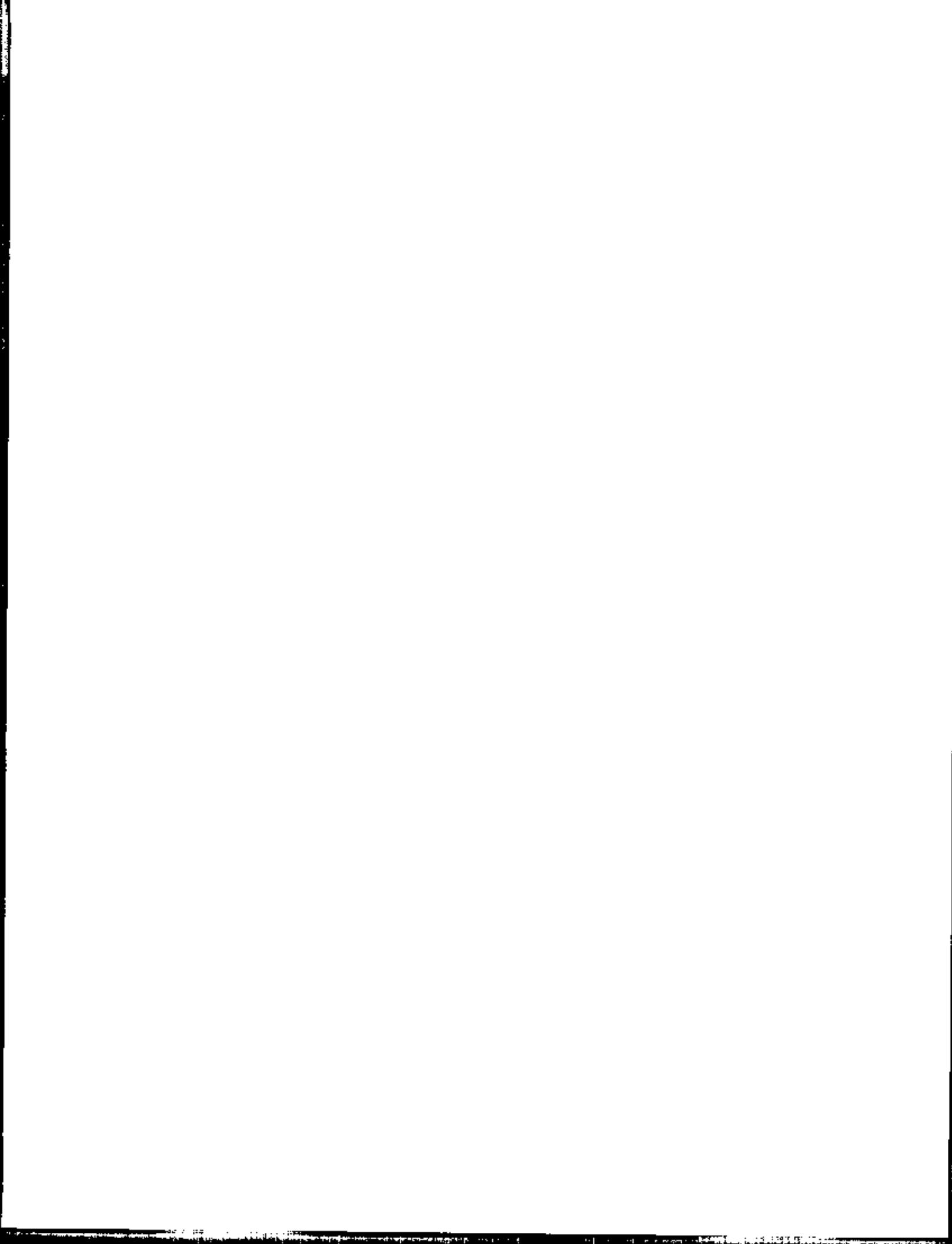
FIRST ENDORSEMENT

From: Security Manager
To: Disposal Unit Officer
Via: Camp Supply Officer, HQSVCBn

1. I hereby verify that the enclosed tapes have been declassified and are ready for destruction.

(Signature)

Figure 17-1.--Format for Certificate of Declassification
of Classified Magnetic Tapes



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

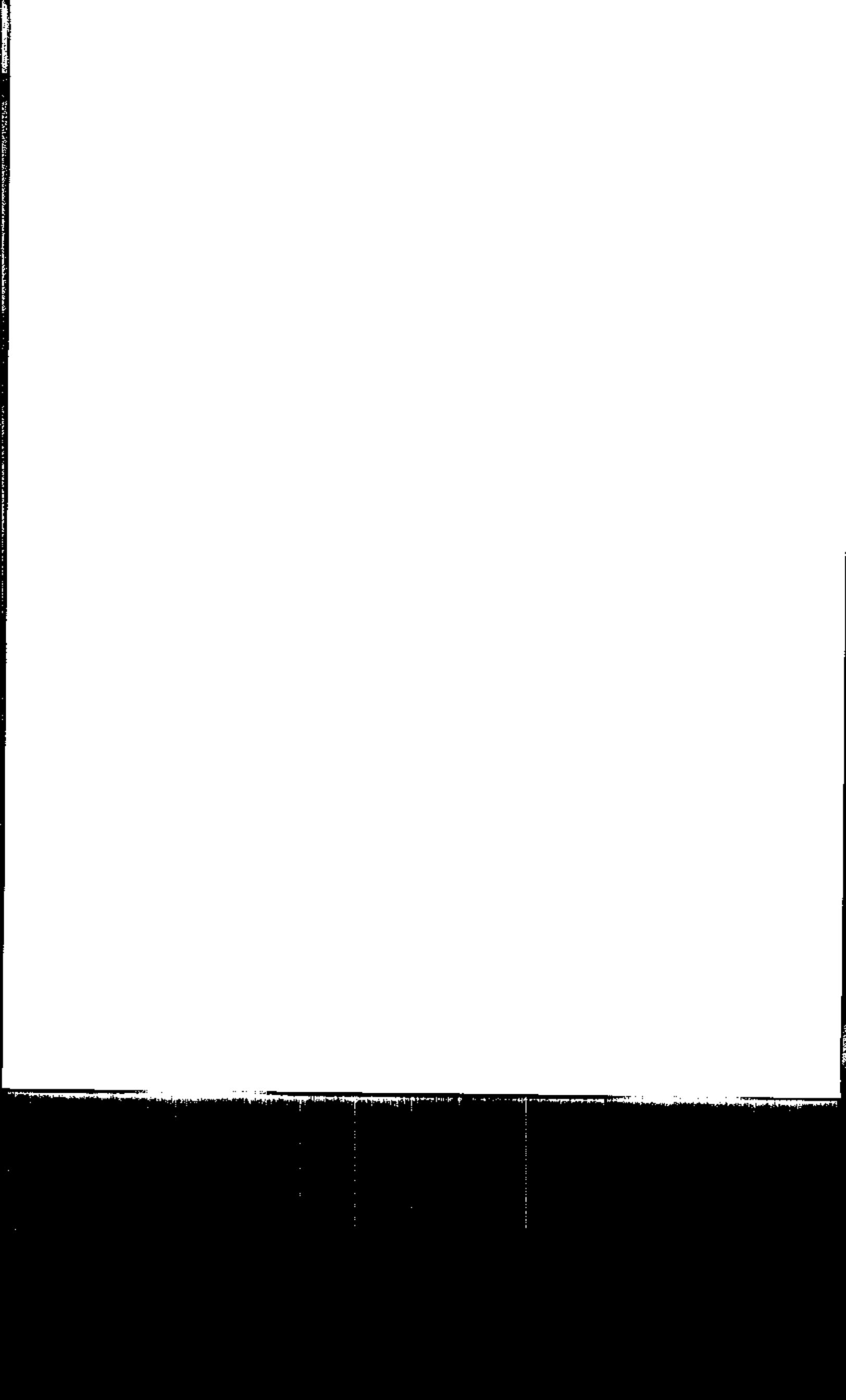
CHAPTER 18

VISIT CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	18000	18-3
VISIT REQUESTS RECEIVED BY THIS HEADQUARTERS.	18001	18-4
VISITS BY FOREIGN NATIONALS	18002	18-4

FIGURE

18-1	VISIT REQUEST/VISITOR CLEARANCE DATA.	18-5
18-2	FORMAT OF A VISIT REQUEST	18-6
18-3	FORMAT OF ACCESS APPROVAL FOR VISITORS.	18-7



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 18

VISIT CONTROL

18000. BASIC POLICY. For security purposes, the term "visitor" applies to all individuals who are not permanently assigned to this headquarters or Camp H. M. Smith. This includes individuals who are in a TAD status of less than 30 days.

1. Division and separate branch heads are responsible for visitors to their respective sections and for ensuring the safeguarding of classified information under their jurisdiction.
2. The movement of all visitors will be restricted to protect classified information. When escorts are used, they must ensure that visitors have access only to information they have been authorized to receive.
3. As a matter of convenience and courtesy, flag officers, general officers, and their civilian equivalents are not required to sign visitor records or display identification badges when being escorted. The escort should be present at all times when the visitor is in sensitive areas of this headquarters.
4. All divisions and separate branches will institute visitor logbook procedures which will serve as a record of all visitors to the section. All visitors will be requested to complete the visitor logbook. If an individual refuses, then the individual will not be permitted within the requested area and the Security Manager will be notified. The log book will contain the date, time, complete name of the individual visiting the command, the individual being visited and the reason for the visit.
5. General visiting by the public will only be allowed on an unclassified basis only, i.e., no classified areas or information will be shown or divulged to the general public. Extra care will be taken to prevent access to spaces containing classified or sensitive equipment unless the equipment has been concealed and/or adequately protected. General visiting by the public will be conducted and monitored based on the probable presence of foreign agents among the visitors.
6. All visits which require access to classified information will be approved prior to the visit by forwarding appropriate clearance information to the Security Manager. Individuals are not permitted to handcarry authorization for such visits and the certification of a clearance in TAD orders is not sufficient to permit access to classified material. All visits requiring access to classified information will be verified and approved by the Security Manager

prior to the visit or release of classified information. There are no waivers to this requirement. No visitor will be given access based solely on a clearance and a need to know must also be established.

7. When a visitor expresses an unusual interest in information they are not authorized to receive or expresses feelings harmful to the best interest of the U.S., the Security Manager will be notified.

18001. VISIT REQUESTS RECEIVED BY THIS HEADQUARTERS. All visit requests received will be forwarded to the Security Manager for appropriate action. Normally, a visit request will be on an OPNAV Form 5521/27, figure 18-1. Figure 18-2 contains the format that will be used by the Security Manager for staffing visit requests. Figure 18-3 is the format which will be used to formally authorize visitor access to classified material.

18002. VISITS BY FOREIGN NATIONALS

1. Policy and procedures for visits by foreign nationals are described in detail in the current edition of OPNAVINST 5510.48.
2. Policy and procedures for visits of nationals from Communist controlled countries are contained in the current edition of OPNAVINST C5510.159.
3. All visits by foreign nationals to this headquarters, to include visits for Protocol purposes, will be reported to the Security Manager via the visitors list published weekly by the Protocol Office.

**SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM**

U.S. GPO: 1985-0-505-441/40000

VISIT REQUEST VISITOR CLEARANCE DATA OPNAV 5521/27 (REV. 1-75) 81N 0107 - LF - 065 - 2235 (CURRENT EDITION OF OPNAVINST. 5518.1 FOR DETAILED INSTRUCTIONS)	PRIVACY ACT STATEMENT ON REVERSE	CHECK ONE <input type="checkbox"/> REPLY REQUIRED <input type="checkbox"/> REPLY ONLY IF NEGATIVE
FROM (COMPLETE ADDRESS OF REQUESTING ACTIVITY) FOLD ON THIS LINE	DATE OF REQUEST SPECIFIC PERSONNEL OR SECTION OF COMMAND TO BE VISITED	
DURATION OF VISIT (ARRIVE)	(DEPART)	DEGREE OF ACCESS REQUIRED
PURPOSE OF VISIT /REMARKS (IF THE VISIT IS TO A CONTRACTOR FACILITY, INCLUDE CONTRACT NUMBER IF APPROPRIATE)		

NAME, RANK, 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	
NAME, RANK AND TITLE OF OFFICIAL AUTHORIZING VISIT AND CLEARANCE		SIGNATURE	
COPY TO:			

Figure 18-1.--Visit Request/Visitor Clearance Data.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

Date

MEMORANDUM

From: Assistant Chief of Staff, G-1 (Security Manager)
To:

Subj: VISIT REQUEST

1. Attached is a visit request, the subject of which falls within your cognizance. Please indicate, by return endorsement, your recommended approval or disapproval of the visit.

(Signature)

Date

FIRST ENDORSEMENT

From:
To: Assistant Chief of Staff, G-1 (Security Manager)

1. It is recommended that the visit request be approved/
disapproved.

Comments:

2. Person/section to be contacted
3. Anticipated level of access required

(Signature)

Figure 18-2.--Format of a Visit Request.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

HEADING

2E
5521
date

From: Commander, Marine Forces Pacific
To:

Subj: APPROVAL OF VISIT REQUEST

1. The personnel listed below are authorized to visit this headquarters for the purposes indicated:

- a. Visitor(s) Security Clearance/Basis and Citizenship:
- b. Company/association:
- c. Date(s) of visit:
- d. Activity and/or person to be contacted:
- e. Level of access authorized:
- f. Purpose of visit:

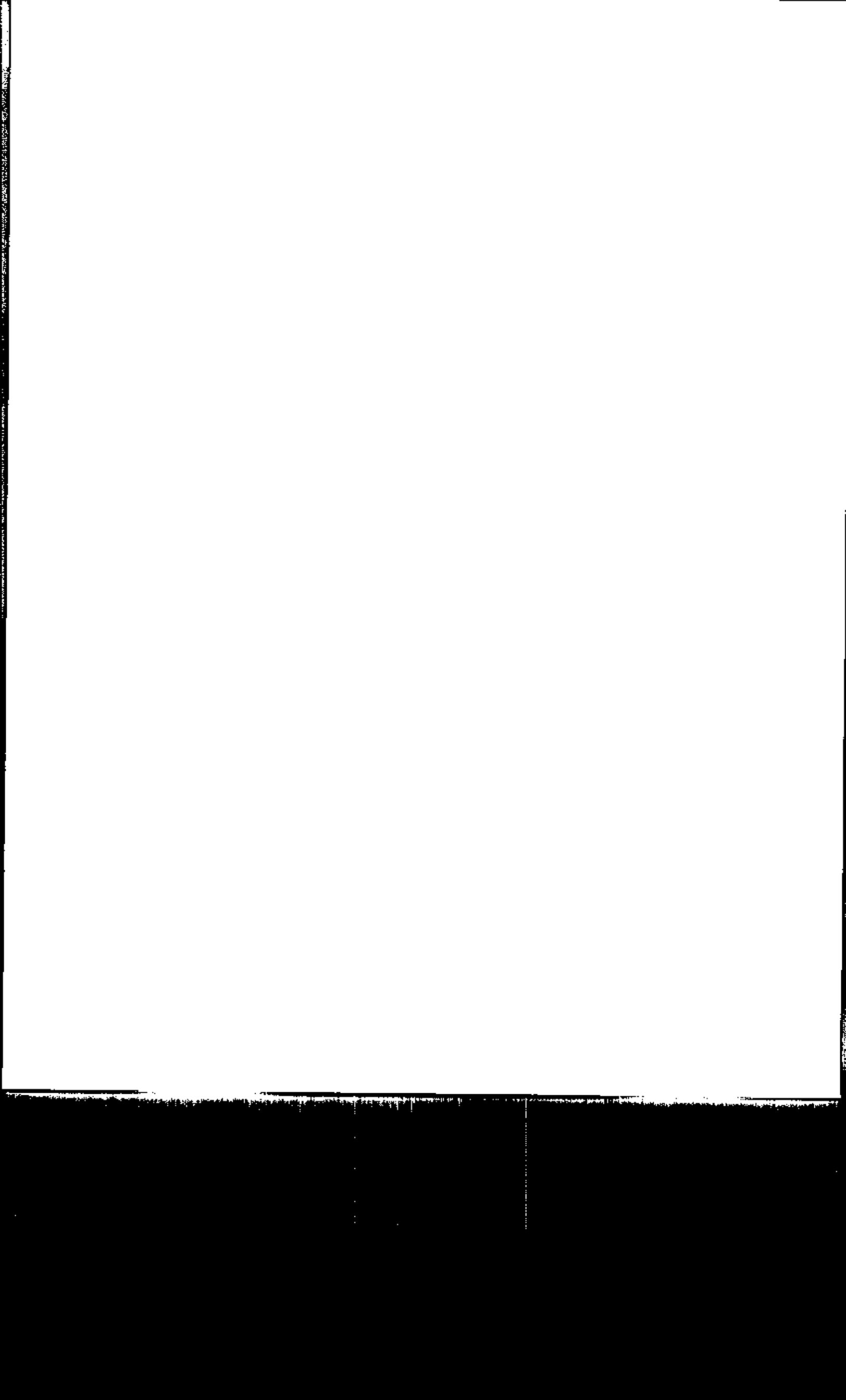
2. The determination to release classified information is the responsibility of the division/branch or staff section to be visited. This determination will be based on the level of access authorized and the visitor's need-to-know.

SIGNATURE

Copy to:
PMO

Figure 18-3.--Format of Access Approval for Visitors.

18-7

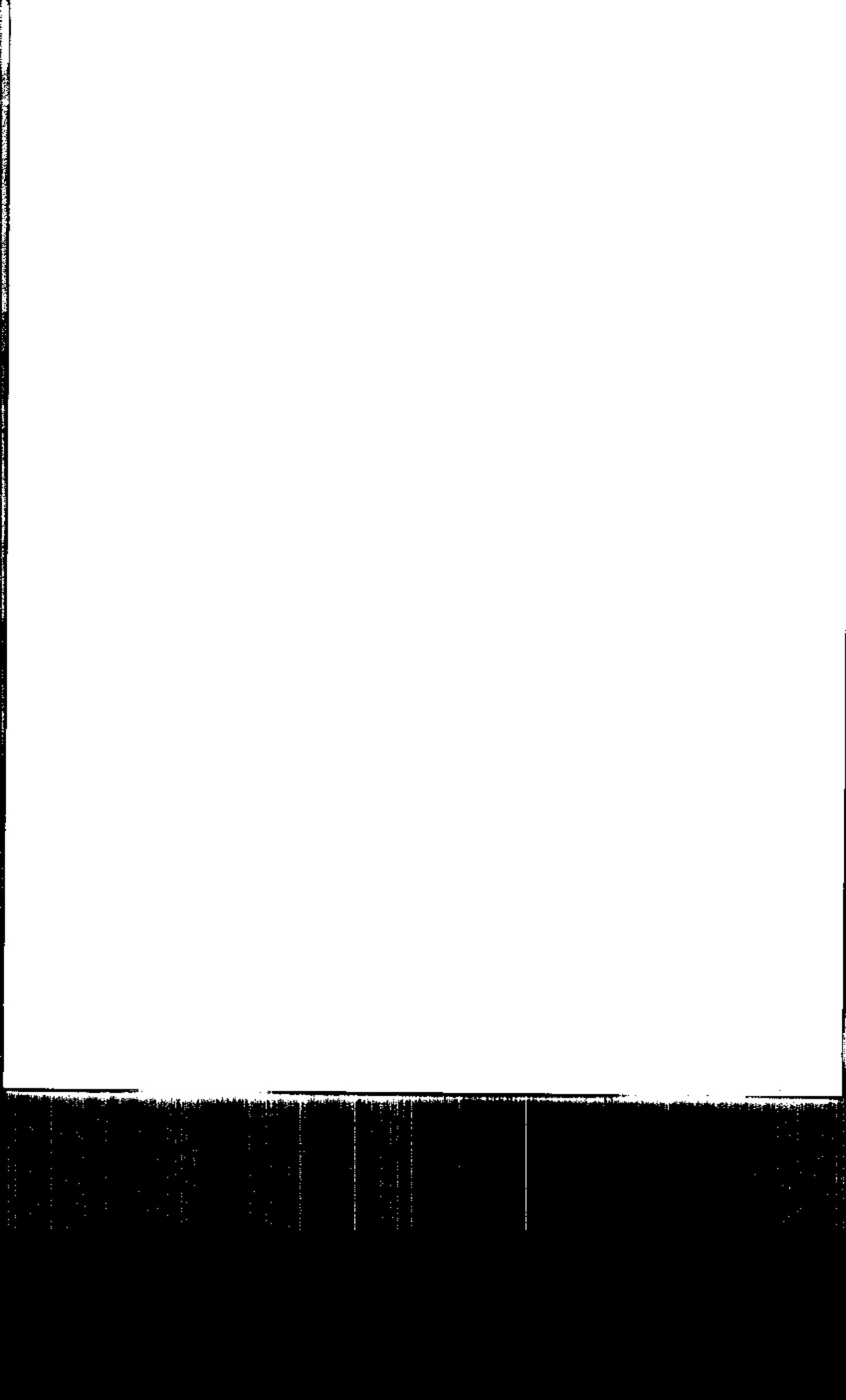


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 19

MEETINGS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	19000	19-3
CLASSIFIED MEETINGS AND CONFERENCES	19001	19-3
CONFERENCES AND MEETINGS INVOLVING FOREIGN NATIONALS	19002	19-3
UNCLASSIFIED MEETINGS AND INSTRUCTIONAL COURSES	19003	19-4



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 19

MEETINGS

19000. BASIC POLICY. Classified information will not be discussed at conferences and meetings under the sponsorship of this headquarters unless approved in writing by the Security Manager.

19001. CLASSIFIED MEETINGS AND CONFERENCES

1. All meetings and conferences, where classified information is to be discussed, will only be conducted in approved U.S. Government controlled facilities.
2. Divisions and separate branches will notify the Security Manager, in writing, of the intent to sponsor a classified conference at least 30 days prior to the conference. Conferences involving Top Secret information will be handled on a case-by-case basis.
3. Security of conference facilities remains the responsibility of the sponsoring division/branch and is not the responsibility of the Security Manager.
4. Clearance, access rosters and access control measures are the responsibility of the sponsoring division or branch. Differences in clearance and access rosters will be resolved with the Security Manager prior to permitting access to the conference. All clearances on personnel not assigned to this headquarters will be verified and certified by the Security Manager. Clearance data on TAD orders is not adequate for granting access to classified information.
5. Classified documents will not be distributed for retention by conference attendees at conferences sponsored by this headquarters. All classified documents will be disseminated per chapter 15 of this Manual.

19002. CONFERENCES AND MEETINGS INVOLVING FOREIGN NATIONALS

1. Personnel from this headquarters will not disclose classified information in meetings involving foreign nationals. If classified information is inadvertently disclosed, the provisions of chapter 4 of this Manual will be complied with.
2. Many foreign nationals attend protocol functions aboard Camp H. M. Smith. Personnel must be aware of the security problems

associated with such visits and should be cautious concerning the disclosure of sensitive military information. All attempts to illicit sensitive information by foreign nationals attending protocol functions will be referred to the Security Manager for appropriate action.

3. The Security Manager will be notified, in writing, of all foreign nationals who will attend meetings and conferences sponsored by this headquarters. This notification will also provide the complete identification of the foreign national.

19003. UNCLASSIFIED MEETINGS AND INSTRUCTIONAL COURSES

1. Occasionally, private companies, educational institutions and individuals conduct unclassified meetings and instructional courses on subjects which are considered sensitive. MARFORPAC personnel occasionally participate as instructors, discussion leaders or attendees at such meetings. When the subjects covered are in the area of sensitive information and operations and the participants have access to classified information, the environment is fertile for inadvertent disclosure of classified information.

2. All personnel scheduled to participate in such meetings or instructional courses are required to report to the Security Manager for an appropriate security awareness briefing.

3. Guidance as to the categories of information requiring security review and the administrative procedures for providing the information for review, are found in the current editions of SECNAVINST 5720.42 and MCO 5510.9. All such submissions will be processed through the Security Manager.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 20

PERSONNEL SECURITY POLICY

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	20000	20-3
APPLICABILITY	20001	20-3
CITIZENSHIP	20002	20-3
VERIFICATION OF CITIZENSHIP	20003	20-3
DESIGNATION OF CIVILIAN SENSITIVE POSITIONS .	20004	20-3

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 20

PERSONNEL SECURITY POLICY

20000. BASIC POLICY. The CO HQSVCBn is responsible for administering the personnel security program within this headquarters. The MARFORPAC Security Manager advises the CO HQSVCBn concerning personnel security matters relative to MARFORPAC and is the principle staff officer for the Personnel Security Program.

20001. APPLICABILITY

1. The personnel security policies and procedures in this Manual apply primarily to the eligibility for access to classified information or assignment to sensitive duties that are subject to investigation under the provisions of this Manual.

2. Detailed requirements for specific programs are found in the regulations governing those special access programs.

20002. CITIZENSHIP. Only U.S. citizens will be granted clearances and access to classified information or assigned to sensitive duties. Immigrant aliens will not be granted access to classified information unless it is in the national interest to do so and a compelling need exists. The final decision rests with the Security Manager.

20003. VERIFICATION OF CITIZENSHIP. Citizenship status affects investigative requirements, clearance eligibility and access; therefore, it must be considered before security processing begins. Citizenship will be verified per paragraph 20-5 of OPNAVINST 5510.1H before initiating any clearance action.

20004. DESIGNATION OF CIVILIAN SENSITIVE POSITIONS

1. Within this headquarters, each civilian position will be designated as critical-sensitive, non-critical sensitive or non-sensitive.

2. The criteria to be applied in designating a position as sensitive are:

a. Critical-sensitive:

(1) Access to Top Secret information.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

(2) Development or approval of plans, policies or programs that affect the overall operations of the DON.

(3) Development of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(4) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations or the making of personnel security determinations.

(5) Fiduciary, public contact or other duties demanding the highest degree of public trust.

(6) Duties requiring access to SCI.

(7) Category I-Automatic Data Program positions. (NOTE: This criterion will not be used to designate a position as critical-sensitive until further notice.)

(8) Any other position designated by the Secretary of the Navy or individual designees (commanding officers).

b. Noncritical-sensitive:

(1) Access to Secret or Confidential information.

(2) Assignment to security police/provost marshal duties involving the enforcement of law and security duties involving the protection and safeguarding of DON personnel or property.

(3) Assignment to duties involving education and orientation of DON personnel. (Applicable only to personnel who prepare formal instructional material or present formal courses of instruction.)

(4) Duties involving the design, operation or maintenance of intrusion detection systems deployed to safeguard personnel and property.

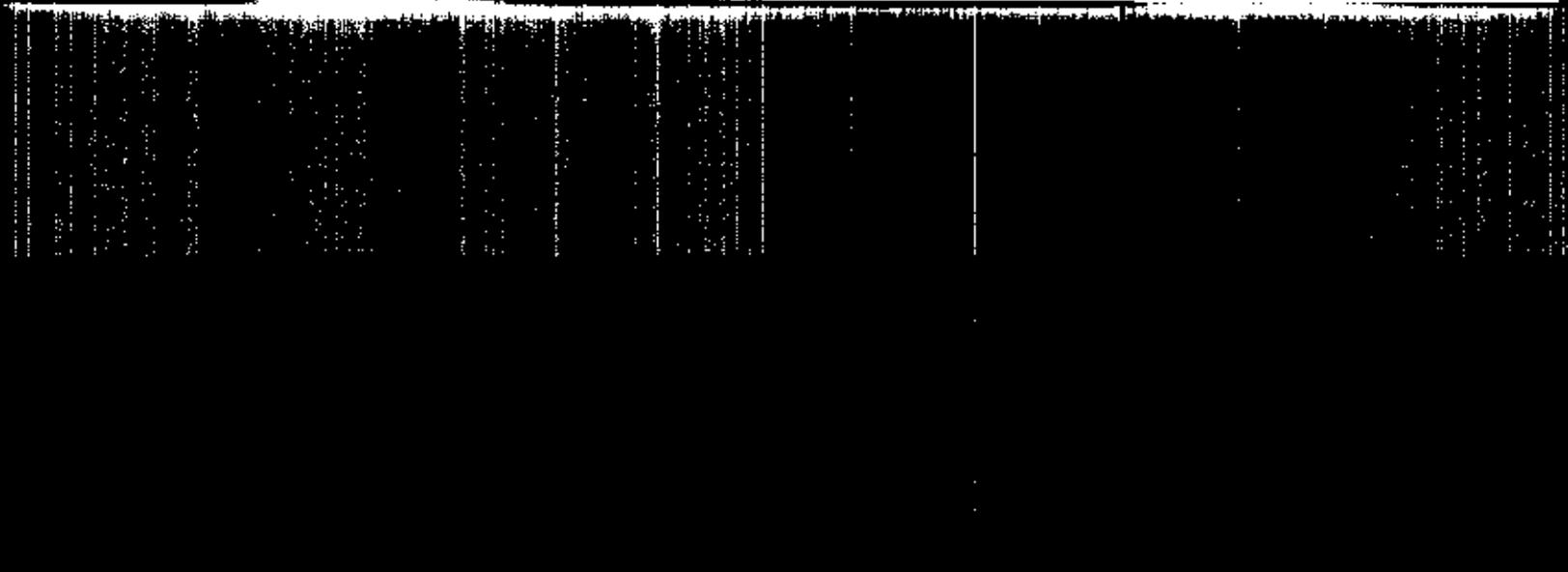
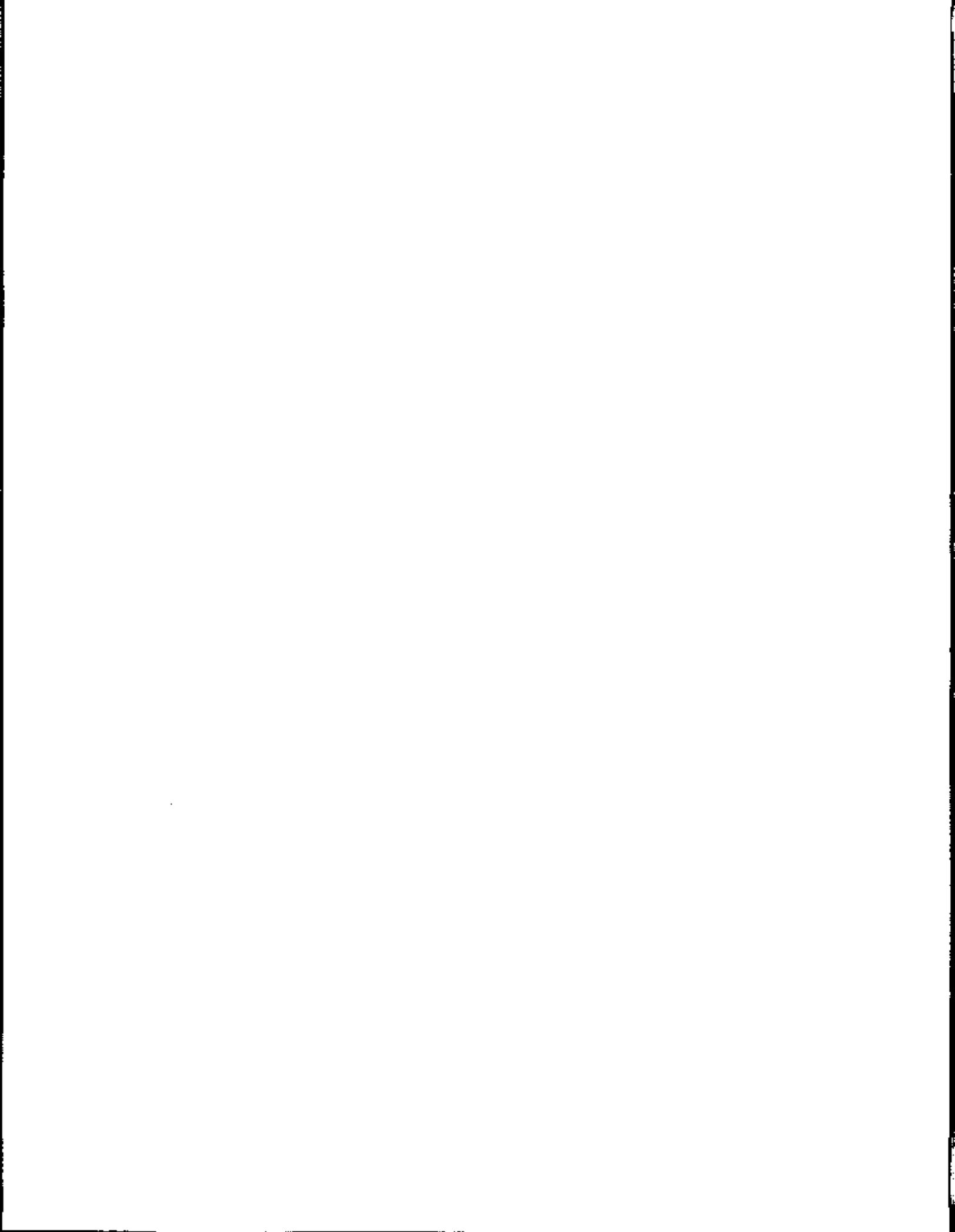
(5) Category II-Automatic Data Program positions.

(6) Any other position designated by the Secretary of the Navy or individual designees (commanding officers).

3. Any one of the criteria will make a position sensitive. If more than one applies, only the predominant factor needs to be recorded. If access to classified information is one of the

factors, it will always be predominant.

4. All other civilian positions are to be designated as non-sensitive. Non-sensitive positions are not under the purview of this Manual.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 21

PERSONNEL SECURITY INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	21000	21-3
TYPES OF PERSONNEL SECURITY INVESTIGATIONS.	21001	21-3
INVESTIGATIVE REQUIREMENTS.	21002	21-4
REINVESTIGATIONS.	21003	21-4
REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS.	21004	21-4
PREPARATION AND SUBMISSION OF INVESTIGATION REQUESTS.	21005	21-4
FOLLOW-UP ACTIONS ON INVESTIGATION REQUESTS	21006	21-4
REPORTS OF INVESTIGATIONS	21007	21-5
VALIDITY OF PRIOR PERSONNEL SECURITY INVESTIGATIONS.	21008	21-7
VERIFICATION OF PRIOR INVESTIGATION	21009	21-7
REQUESTS FOR PRIOR INVESTIGATIVE FILES.	21010	21-7

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 21

PERSONNEL SECURITY INVESTIGATIONS

21000. BASIC POLICY

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable determination has been made of their loyalty, reliability, trustworthiness and judgement. The initial determination will be based on a personnel security investigation (PSI) appropriate to the access required or to other considerations of the sensitivity of the duties assigned.
2. The CO HQSVCBn is authorized to request PSIs on personnel under the CO's jurisdiction as is necessary to fulfill the investigative requirements described in this chapter.
3. Only the minimum investigation to satisfy a requirement may be requested.
4. The Defense Investigative Service (DIS) or the Office of Personnel Management (OPM), conducts or controls all PSIs for the DON. The commanding officer is prohibited from conducting PSIs, including local public agency inquiries, without the specific request from the DIS to support its investigative responsibilities.
5. Requests for PSIs must be kept to the absolute minimum. Special attention is to be given to eliminating unnecessary and duplicate requests. An investigation will not be requested to resolve allegations of a suitability nature for the purpose of supporting personnel administrative decisions or disciplinary procedures independent of a personnel security determination.

21001. TYPES OF PERSONNEL SECURITY INVESTIGATIONS. The term "Personal Security Investigation (PSI)" describes an inquiry by an investigative agency into an individual's activities, and is conducted for the purpose of making a personnel security determination. Other types of investigations may have an impact on employment, clearance or assignment but are conducted for other basic purposes and are, therefore, not PSIs. Examples of other types are investigations of compromise, current criminal activity, sabotage, espionage or subversion. The various types of personnel security investigations are described in paragraph 21-2 of OPNAVINST 5510.1H.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

21002. INVESTIGATIVE REQUIREMENTS. Investigative requirements for civilian employment, military appointment, access to classified information by U.S. citizens/non-U.S. citizens, SCI, SIOP, NATO or foreign-oriented information, personnel reliability program, presidential support activities or other specific performance of duties are contained in chapter 21 of OPNAVINST 5510.1H. All personnel who have a Top Secret clearance will have a periodic reinvestigation every five years.

21003. REINVESTIGATIONS. Reinvestigations of an individual who has already been investigated will only be approved by the Security Manager under the conditions described in paragraph 21-13 of OPNAVINST 5510.1H.

21004. REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS

1. All requests for PSIs will be provided to the Security Manager for validation and approval. The CO will not request a PSI on an individual until it has been validated and approved by the Security Manager.

2. All PSIs for access to SCI will be validated and approved by the SSO. Each nominee for SCI must be personally interviewed by the SSO. Clerical personnel within the SSO are not authorized to conduct the interview.

3. The CO must personally validate the request for an SBI on an immigrant alien and sign the DD Form 1879 stating "Investigation required to meet essential requirements of the Marine Corps". Paragraph 20002 of this Manual identifies citizenship requirements for security clearances within this headquarters.

21005. PREPARATION AND SUBMISSION OF INVESTIGATION REQUESTS. The CO HQSVCBn is responsible for the administrative preparation and submission of all forms associated with the PSIs under the personnel security program. The SSO will review investigative packages being provided on personnel for SCI access. The individual who is the subject of a PSI will prepare all necessary forms in a "rough draft" and provide them to HQSVCBN (S-1) in a timely manner.

21006. FOLLOW-UP ACTIONS ON INVESTIGATION REQUESTS

1. If the investigation request is rejected by the investigative agency because the forms were not completely or properly executed and an investigation is still required, corrective action will be

taken and the request resubmitted. All of the forms being resubmitted and a copy of the request form which was placed in the official personnel record, are to be annotated with the resubmission date. If the subject has been transferred, the request package will immediately be forwarded to the gaining command for correction and resubmission.

2. If an investigation is in a pending status and the subject is released from active duty, is discharged or resigns, the investigation is to be promptly cancelled. If an individual is transferred from this headquarters, allow the investigation to proceed unless it is evident that the investigation will not be required after transfer.

3. When an individual is transferred after an SBI has been requested, the losing command will notify DIS of the proper recipient of the results of the investigation. DIS will be notified by a corrected copy of the DD Form 1879. (This procedure is not required for NACIs, NACs or ENTNACs.)

4. If results of an investigation are not received within a reasonable time, tracer action may be initiated. Tracer action on a NAC or ENTNAC should not be taken until 60 days after submission of the investigation request. NACI tracers should not be sent until 90 days after submission of the investigation request. Tracer action will not be initiated until 90 days after submission of a request for a BI or SBI. Requests for the status of an SBI for access to SCI will not be directed to Commander, Naval Intelligence Command or Commander, Naval Security Group Command until 120 days after submission of the request and only after coordination with the SSO. Tracer action is accomplished by forwarding, to the investigative agency, a copy of the request form which had been placed in the official personnel record with the word TRACER printed or stamped in large letters across the face of the form.

5. In cases where an individual was given an Interim Top Secret clearance pending the completion of the investigative requirements, the CO will initiate tracer action at the end of six months, annotate the OPNAV Form 5520/20 and notify the MARFORPAC Security Manager. Additional tracer action will be provided in 30 day intervals until the investigation is completed.

21007. REPORTS OF INVESTIGATIONS

1. In recognition of the sensitivity of personnel security reports and records, particularly with regard to personal privacy, results of investigations will be handled with the highest degree of discretion. Control and safeguard the results of investigations as

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

described below unless the results are reported as clearly favorable with no investigative material attached; or by stamped endorsement on the DD Form 1879; or by Report of NAC/ENTNAC with all agencies checked with favorable results. Any report of an investigation which includes investigative material, favorable or unfavorable, must be handled, stored and transmitted per the safeguards described.

a. Investigative reports are to be made available only to those authorities who require access in the performance of their official duties for the purposes of determining eligibility for access to classified information, assignment to sensitive duties, acceptance or retention in the Armed Forces, appointment or retention in civilian employment or for law enforcement and counterintelligence purposes. Destroy all copies of PSIs as soon as final action is taken. Retention of PSIs longer than 120 days after final action has been completed must be specifically approved, in writing, by the investigating agency.

b. Investigative reports will be stored in a vault, safe or steel filing cabinet having at least a lockbar and an approved, three-position, dial-type combination padlock, or in a similarly protected container or area.

c. Reports of investigation will not be shown to the subject of the investigation without the specific approval of the investigating agency. Under no circumstances will reports of an investigation be placed in the subject's official personnel record.

d. When being transmitted by mail or carried by persons not authorized access, reports of an investigation will be sealed in double envelopes and bear a notation of whom is to receive the report or investigation. The inner container is to be opened only by an official of personnel security investigations.

2. If the results of an investigation are received at this headquarters after the subject has been transferred, forward the results to the gaining command.

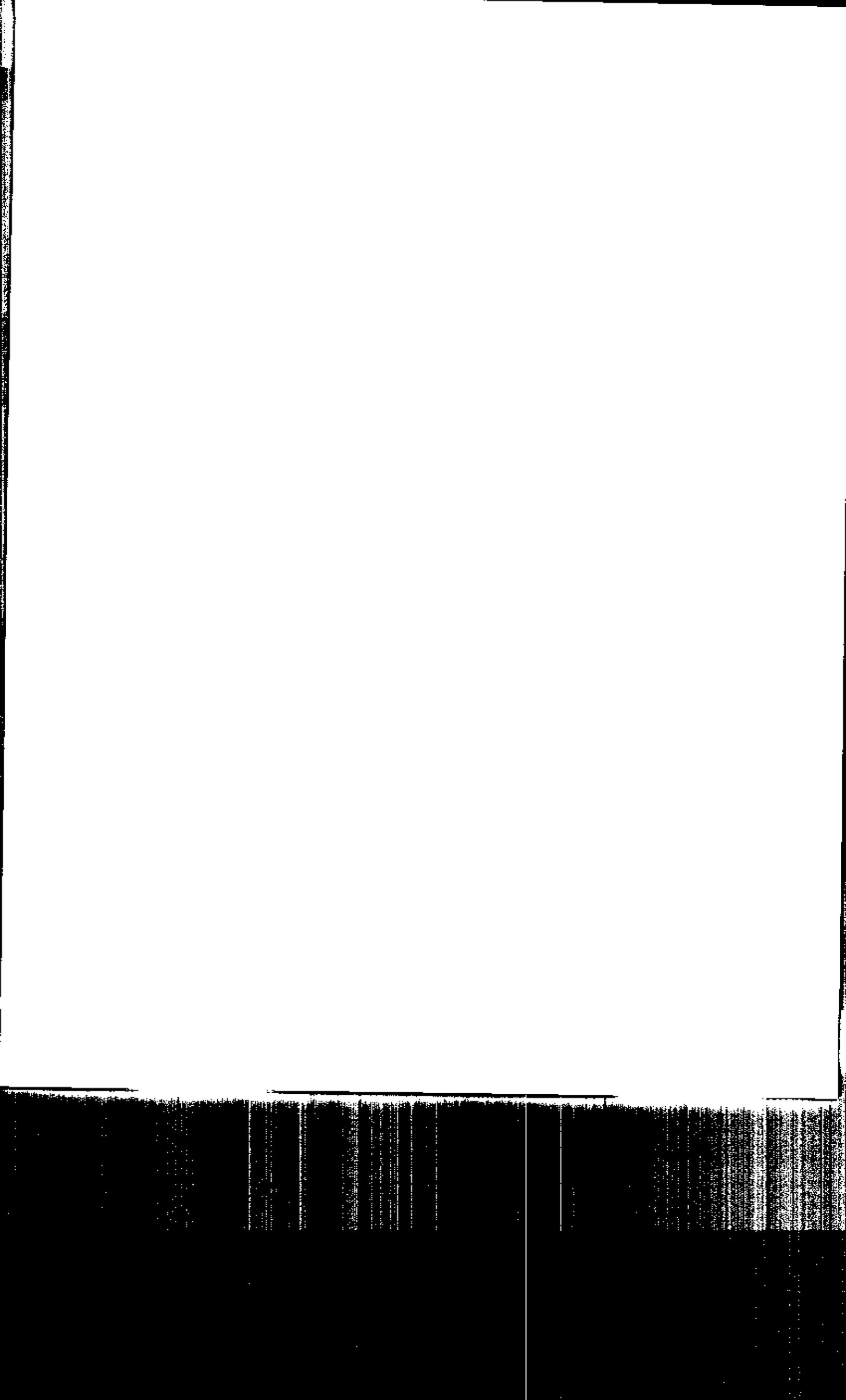
3. Record completed PSIs on the Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20). The adjudication of the investigation will also be recorded under the procedures in chapter 22 of this Manual for recording personnel security determinations.

4. All adverse or unfavorable actions taken by this headquarters, based on the results of a DIS investigation, will be reported to DIS.

21008. VALIDITY OF PRIOR PERSONNEL SECURITY INVESTIGATIONS. In determining the validity of prior personnel security investigations, the factors described in paragraph 21-18 of OPNAVINST 5510.1H will be used as a guide. If any conflict exists, the Security Manager will be notified prior to initiating an additional PSI.

21009. VERIFICATION OF PRIOR INVESTIGATION. When there is no valid certification of clearance or documentation of completed investigation in the record, but there are clear indications that prior investigation has been conducted which would still be valid for current needs, the CO will request verification of the prior investigation from the Director, Naval Investigative Service. Telephone verification is not an acceptable basis for entries on the Certificate of Personnel Security Investigation, Clearance, and Access (OPNAV 5520/20).

21010. REQUEST FOR PRIOR INVESTIGATIVE FILES. Requests for prior investigative files on MARFORPAC personnel will not be acknowledged unless approved by the Security Manager.

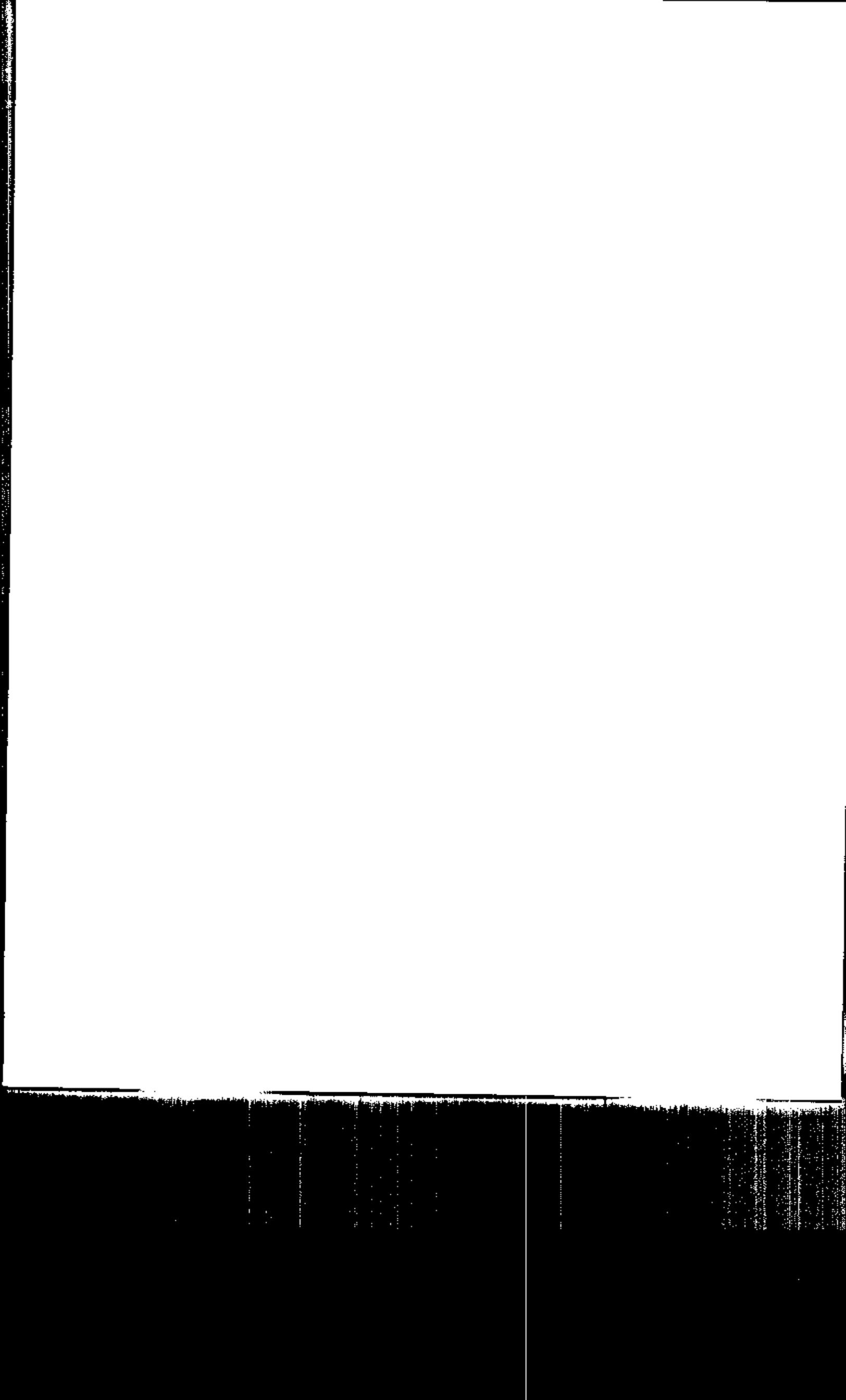


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 22

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	22000	22-3
SECURITY CRITERIA	22001	22-4
PERSONNEL SECURITY DETERMINATION AUTHORITY . .	22002	22-4
PERSONNEL SECURITY DETERMINATIONS	22003	22-5
ADVERSE PERSONNEL SECURITY ACTIONS.	22004	22-5
ADVERSE PERSONNEL SECURITY DETERMINATION PROCEDURES.	22005	22-6
VALIDITY AND RECIPROCAL ACCEPTANCE OF PERSONNEL SECURITY DETERMINATIONS.	22006	22-6
CONTINUOUS EVALUATION OF ELIGIBILITY.	22007	22-7



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 22

PERSONNEL SECURITY DETERMINATIONS

22000. BASIC POLICY

1. The principal objective of personnel security determinations is to ensure that the loyalty, reliability, judgement and trustworthiness of those with access to classified information or those assigned to sensitive duties, are such that entrusting them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security.
2. The personnel security determination of eligibility for access to classified information or assignment to sensitive duties requires a common sense evaluation of all available information about the individual. All information, favorable and unfavorable, will be considered and assessed in terms of accuracy, completeness, relevance, seriousness and overall significance.
3. A determination to grant security clearance or to assign an individual to sensitive duties will be based, as a minimum, on a PSI or check per the requirements specified for various levels or kinds of access, positions or duties.
4. Determinations of suitability or eligibility for civilian employment or military service are not personnel security determinations unless loyalty is the central issue.
5. Marine personnel assigned to MARFORPAC will have their appropriate security clearances entered into the MMS by the MARFORPAC security clerk. Navy personnel assigned to MARFORPAC will have their security determinations documented on the Certificate of Personnel Security Investigation, Clearance and Access (OPNAV Form 5520/20), as required by exhibit 22A of OPNAVINST 5510.1H.
6. For naval personnel assigned, each time a final clearance action or other documentation of a personnel security determination is entered on OPNAV Form 5520/20 for an individual, a copy of the form must be sent to Commander, Naval Military Personnel Command (NMPC-81). For Marine personnel, an entry will be entered into the MMS.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM22001. SECURITY CRITERIA

1. The personnel security determination required by paragraph 20001 and this paragraph will be an overall, common sense determination based on all available information. In arriving at the determination, certain activities and associations of varying degrees of seriousness, current or past, warrant appropriate investigation and careful consideration.
2. Paragraph 22-2 of OPNAVINST 5510.1H provides a listing of various factors to be evaluated in making a personnel security determination.
3. CI assistance is available through the Security Manager in making decisions relative to personnel security matters.

22002. PERSONNEL SECURITY DETERMINATION AUTHORITY

1. The authority to determine eligibility for access to classified information or to deny appointment or retention in employment of civilian personnel for loyalty reasons, is vested solely in the Secretary of the Navy.
2. Personnel security determination on military personnel within this headquarters rests with the CO HQSVCBn, with the exception of access to SCI. These determinations include adjudication of investigations and the granting or denying of clearances.
3. Personnel security determinations on civilian personnel rests with the Director, Naval Civilian Personnel Command, with input from the MARFORPAC Security Manager.
4. The Director of Naval Intelligence (DNI), as the senior official of the intelligence community for the DON, has been designated by the Secretary of Defense as the official authorized to grant, deny or revoke access to SCI. Under procedures established by the DNI, Commander, Naval Intelligence Command and Commander, Naval Security Group Command have been delegated authority to:
 - a. Adjudicate personnel security investigations and relevant information on all nominees for access to SCI.
 - b. Grant, deny or revoke access to SCI.

22003. PERSONNEL SECURITY DETERMINATIONS

1. A personnel security determination must be made and documented when a personnel security investigation is completed. A personnel security determination is also required when access to classified information or assignment to sensitive duties is necessary under interim or emergency conditions; or questionable or unfavorable information becomes available about an individual on whom a favorable determination had been made; or there are reasonable indications that the factors upon which a previous adverse determination was made no longer exist and the individual is a candidate for clearance or assignment to sensitive duties.
2. A determination must be made when a personnel security investigation is completed; however, an investigation is not the only basis for a determination. All available information must be evaluated by the delegated authority to determine initial and continued eligibility for access to classified information or assignment to sensitive duties. The adjudication guidelines in chapter 22 of OPNAVINST 5510.1H are to be used in evaluating information in PSIs and information available from other sources including personnel, medical, legal and security files. As the basis for a personnel security determination is usually expressed in terms of the investigative requirements, there is sometimes a tendency to discount information acquired about an individual because it isn't documented by an investigation. Eligibility for access or assignment to sensitive duties depends on consideration of all information from any source reflecting on an individual's loyalty, reliability, judgement and trustworthiness. In all adjudications, the protection of national security must be the paramount determinant.
3. Personnel security determinations will be recorded as identified in paragraph 22000.5 of this Manual. A clearance action is not required even though a personnel security determination has been made.

22004. ADVERSE PERSONNEL SECURITY ACTIONS

1. The following constitute adverse personnel security actions, under the provisions of this Manual, when the actions described are based on adverse personnel security determination:
 - a. Denial or revocation of a security clearance.
 - b. Denial or revocation of a Special Access Authorization (including access to SCI).
 - c. Non-appointment to or non-selection for sensitive duties.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

d. Reassignment to duties of lesser sensitivity or to a civilian nonsensitive position.

e. Non-appointment to or termination of civilian employment for loyalty reasons.

f. Non-acceptance for or discharge from the Navy or Marine Corps for loyalty reasons.

2. Military members or civilians will not be removed from employment or separated from the service using this Manual as authority if removal or separation can be effected under administrative (nonsecurity) regulations.

3. Reduce to writing the rationale underlying each adverse personnel security determination. Normally, the statement of reasons and the written final reasons, required by the current edition of MCO 5521.3, will suffice as the rationale.

4. The CO HQSVCBn will determine whether, on the basis of all the facts available and upon receipt of the initial derogatory information, it is in the interests of national security to take interim action to suspend or limit the individual's access to classified information or to assign the individual to other sensitive duties until a final determination is made.

22005. ADVERSE PERSONNEL SECURITY DETERMINATION PROCEDURES

1. The current edition of MCO 5521.3 provides complete guidance on the proper procedures to take in rendering an adverse personnel security determination.

2. If the CO HQSVCBn takes an adverse personnel security action based on a DIS investigation, DIS will be notified for recording the action in the Defense Control Index of Investigation.

22006. VALIDITY AND RECIPROCAL ACCEPTANCE OF PERSONNEL SECURITY DETERMINATIONS

1. A personnel security clearance granted by an authority of the DoD, remains valid and will be mutually and reciprocally accepted within the DoD until:

a. The individual is separated from the Armed Forces or civilian employment, or the individual has no further official relationship with the DoD.

b. The clearance has been officially withdrawn or it has been denied or revoked for cause.

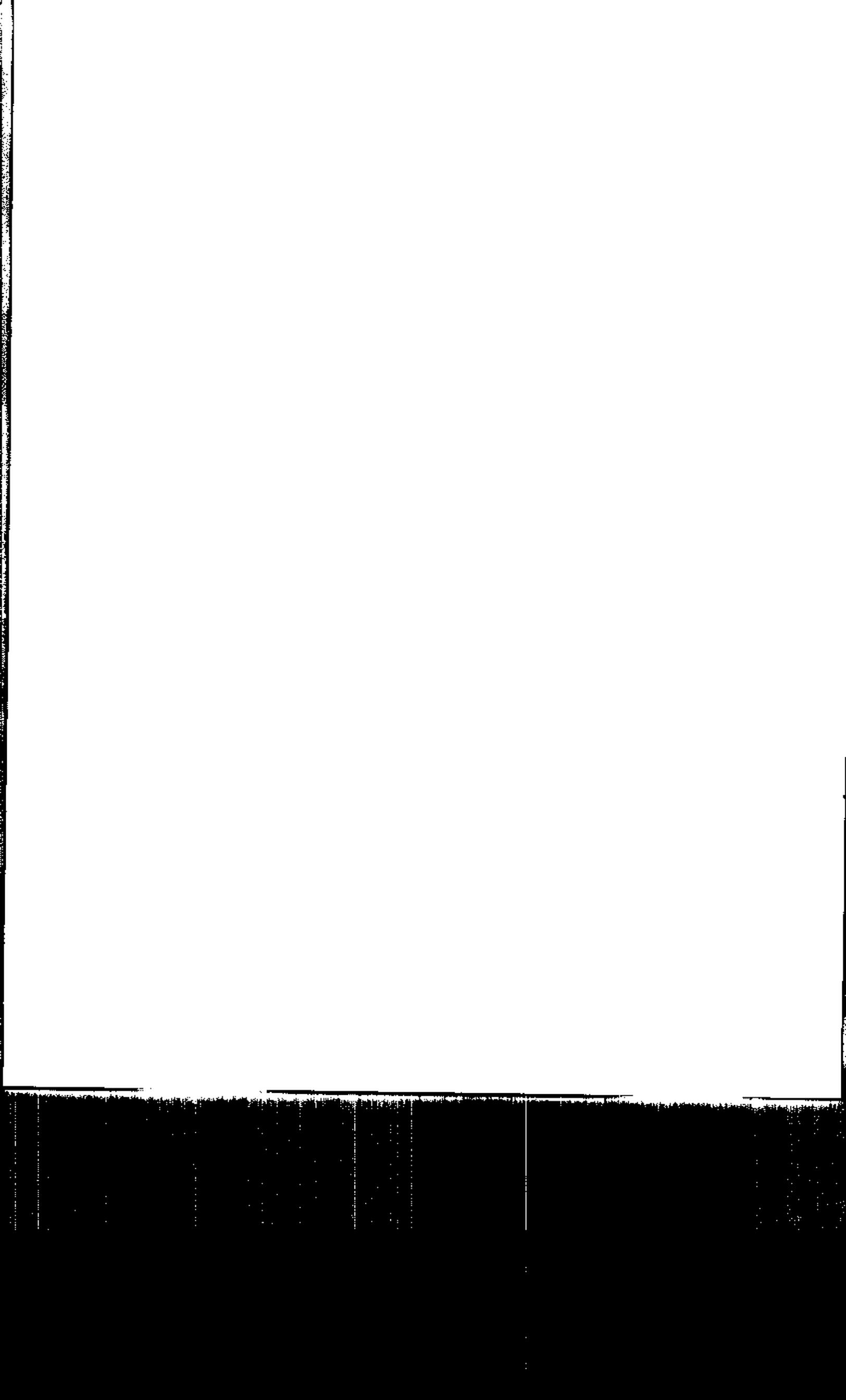
2. The Security Manager will be the determining authority for validating and accepting of other government agency issued security clearances.

22007. CONTINUOUS EVALUATION OF ELIGIBILITY

1. Personnel security responsibilities do not stop once a favorable personnel security determination is made. This headquarters has instituted an aggressive program of continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

2. Under this program, all division and separate branch heads, the CO HQSVCBn and anyone else who is aware of derogatory information on a member of this headquarters, will notify the Security Manager concerning this information. Information in this category includes but is not limited to behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, criminal conduct and any other information which could place an individual's loyalty, reliability, judgement and trustworthiness in question.

3. When derogatory information is developed, the CO HQSVCBn must re-evaluate the individual's eligibility for clearance and access.

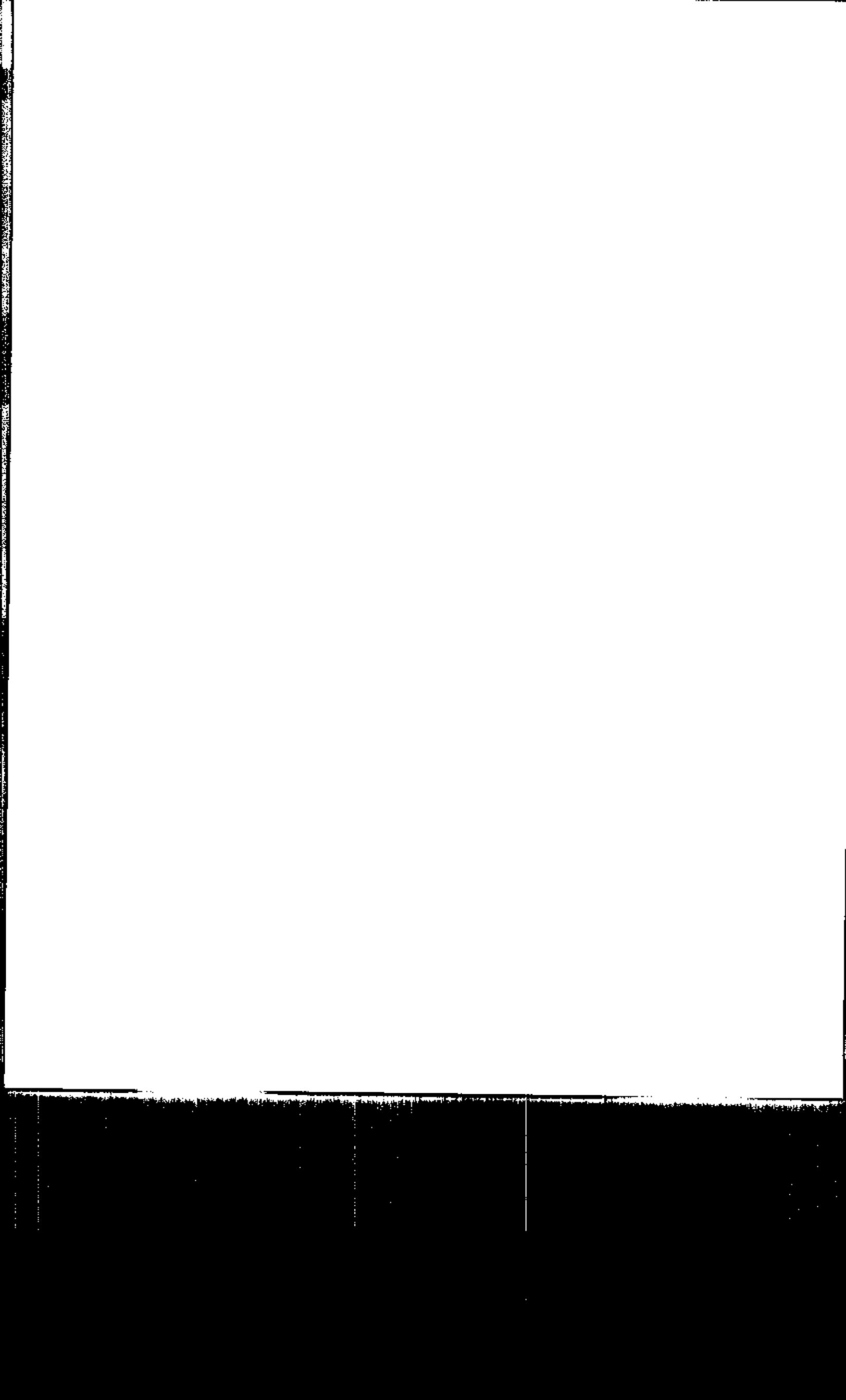


SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 23

CLEARANCE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	23000	23-3
CLEARANCE ELIGIBILITY	23001	23-3
INTERIM AND FINAL CLEARANCES.	23002	23-3
REQUESTS FOR CLEARANCE.	23003	23-4
GRANTING AND RECORDING CLEARANCE.	23004	23-4
NATO SECURITY CLEARANCES.	23005	23-5
ADMINISTRATIVE WITHDRAWAL OF CLEARANCE.	23006	23-6
DENIAL OR REVOCATION OF CLEARANCE FOR CAUSE	23007	23-6



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 23

CLEARANCE

23000. BASIC POLICY

1. As a general rule, personnel security determinations are expressed in terms of eligibility for access to classified information and or security clearance. A security clearance indicates that the person concerned is eligible for access to classified information should their official duties require it. The decision to grant access to classified information is a separate determination based on a need to know (see chapter 24 following).
2. A security clearance will be granted only upon affirmation that clearance is clearly consistent with the interests of national security. Investigative requirements for each level of clearance are specified in chapter 21.
3. Citizenship status will be verified before a security clearance is granted.

23001. CLEARANCE ELIGIBILITY

1. Eligibility for security clearance is limited to military and civilian members of this headquarters, HQSVCBn and Camp H. M. Smith.
2. Individuals not assigned to this headquarters, HQSVCBN and Camp H. M. Smith will not locally be granted a security clearance.
3. Immigrant aliens and foreign nationals will not be granted a security clearance within this headquarters (see paragraph 20003).
4. Reserve personnel in an "active" status are eligible for a security clearance, as required. Normally, a PSI will not be initiated on reserve personnel who are conducting active training of less than 60 days. The clearance authority will be the command holding the service record and exercising administrative jurisdiction over the reservist.

23002. INTERIM AND FINAL CLEARANCES

1. Security clearances are of two types:
 - a. Final clearance - one granted upon completion of all

investigative requirements as set forth in chapter 21.

b. Interim clearance - one granted temporarily, based on the lesser requirement set forth in chapter 21, pending completion of the full investigative requirements. Normally, an interim clearance will not be granted for personnel assigned to this headquarters unless a compelling or emergency situation exists. The final decision whether or not to grant an interim clearance rests with the Security Manager.

2. Interim clearances are effective for six months. Investigation required to effect a final clearance must be requested at the time interim clearance is granted as a condition of the interim clearance. An interim clearance may be extended in six month increments if tracer action confirms that the investigation is still pending. A final clearance will be executed upon satisfactory completion of the investigation.

23003. REQUESTS FOR CLEARANCE. All requests for clearance within this headquarters will be provided to the Security Manager for validation. Requests for clearance will be provided on an individual basis and will not be multiple requests (i.e., three individuals listed on one request).

23004. GRANTING AND RECORDING CLEARANCE

1. Upon receipt of a completed personnel security investigation (including periodic reinvestigation), the CO will adjudicate the results considering all other information available on the individual, and make a personnel security determination to grant or deny clearance. The final action will be recorded as identified in paragraph 22000.5.

2. Clearances will only be granted to the highest level required for access in the performance of official duties, (i.e., Secret access requires Secret clearance, Top Secret access requires Top Secret clearance, etc.). All requests for SCI access require a Top Secret clearance.

3. Clearances will only be granted or lowered based on a request for access which has been validated by the Security Manager.

4. When unfavorable information disclosed in the investigation or is made known to the determining authority results in an adverse personnel security determination, clearance will be denied or granted at a lower level. For Marine personnel, an appropriate MMS entry will be made. For Navy personnel, an entry in the comments section of the OPNAV Form 5520/20 referring to the correspondence

or location in the personnel record or command records where the basis for the adverse determination is documented, i.e., "Clearance terminated per CO HQSVCBn, Camp H. M. Smith, HI ltr 5521 dtd 10 Sep 94".

5. Record interim clearance in the same manner as final. When an interim clearance is based on other than an investigation, indicate the basis for the clearance.

6. Entries on OPNAV Form 5520/20 must be signed by the CO HQSVCBn or other designated clearance authority. Any person authorized to grant personnel security clearances must have been the subject of a BI.

7. The SSO will advise the CO HQSVCBn when a final favorable determination of eligibility for access to SCI or other DON Special Access is received from Commander, Naval Intelligence Command or Commander, Naval Security Group Command. Notification of a final favorable adjudication for SCI access will be accepted as sufficient justification for issuing a final Top Secret clearance. The CO HQSVCBn will ensure that the investigation and clearance are recorded as identified in paragraph 22000.5.

8. Place the Certificate of Personnel Security Investigation, Clearance and Access in the individual's official personnel record and retain it as a permanent, cumulative part of the individual's official record. If the form has been completely filled in, prepare an additional form and attach it to the original. The signature of the authorizing official (the CO HQSVCBn or other designated clearance authority) and the name of the command are required for each clearance action. Facsimiles or carbon signatures are not authorized. Each time a completed investigation or final clearance action is entered, send a signed copy (reproduction or duplicate) to the Naval Military Personnel Command (NMPC 81) for Navy members, or to the Commandant of the Marine Corps (MSRB) for Marine Corps members.

23005. NATO SECURITY CLEARANCES

1. A final U.S. security clearance, or the equivalent level of classification, is the basis for access to NATO classified information. Access to NATO material in this headquarters is described in chapter 24.

2. When additional certification of security clearance is required, use the appropriate format from appendix E or F of OPNAVINST C5510.101.

3. Interim clearances may not be used as the basis for access to NATO information except under emergency conditions requiring immediate action in furtherance of U.S. or NATO purpose. If such a clearance is granted, then the conditions of paragraph 23-7 of OPNAVINST 5510.1H must be complied with.

23006. ADMINISTRATIVE WITHDRAWAL OF CLEARANCE

1. The security clearance of an individual will be administratively withdrawn when there is no foreseeable need for access to classified information in connection with their official duties.

2. When a security clearance is administratively withdrawn, appropriate action as identified in paragraphs 22005/6 will be taken to show that the action was taken administratively and without prejudice to the individual's future eligibility for access. An adverse personnel security determination will result in denial or revocation of clearance.

3. When a clearance is administratively withdrawn, debrief the individual per paragraph 3007 of this Manual and file the executed Security Termination Statement in the official personnel record.

23007. DENIAL OR REVOCATION OF CLEARANCE FOR CAUSE

1. When a personnel security determination has been made that an individual does not meet or no longer meets the criteria for security clearance in paragraph 22002, clearance will be denied or revoked for cause by the determining authority (the CO for military personnel, the Director, Naval Civilian Personnel Command for civilian personnel).

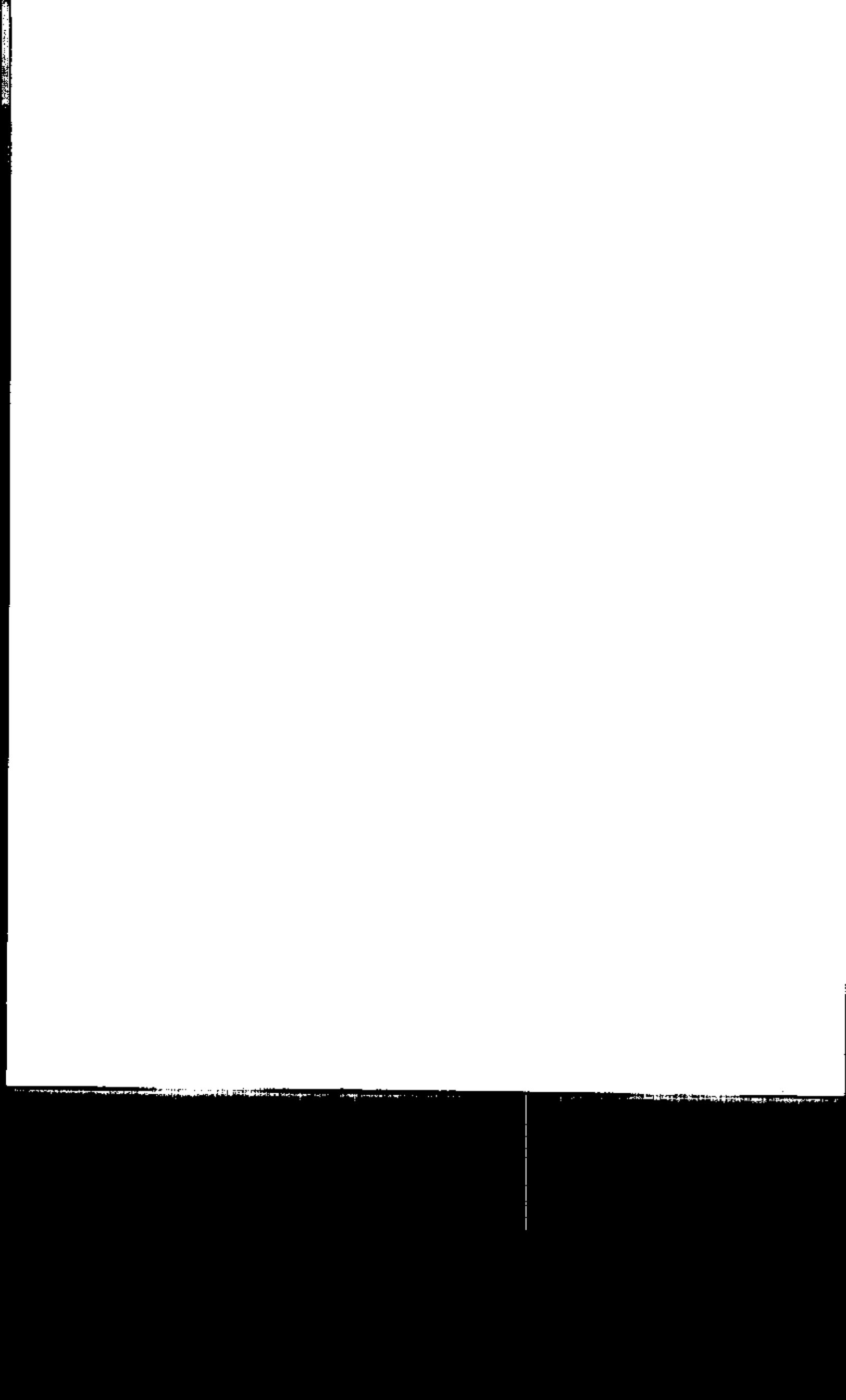
2. Denial or revocation of security clearance for cause is an adverse personnel security determination. On revocations, debrief the individual per paragraph 3007 of this Manual and file the Security Termination Statement in the official personnel record.

3. A decision to grant a clearance at a lower level based on the development of derogatory information, is an adverse personnel security determination. The individual will be advised of this adverse personnel security determination using the same procedures for revoking a clearance.

4. Detailed instructions for processing cases of denial or revocation are contained in the current edition of MCO 5521.3.

5. A security clearance, previously denied or revoked for cause, may be reinstated when it is determined that the individual now

meets the criteria for clearance and a need for clearance exists. The concurrence of the Commander, Naval Military Personnel Command is required before initiating action to reinstate clearance for a Navy member. For a Marine Corps member, the CO HQSVCBn may reinstate clearance without prior concurrence of the Commandant of the Marine Corps. For civilian personnel, a recommendation to grant or reinstate security clearance must be provided to the Director, Naval Civilian Personnel Command for consideration. A recommendation would not be appropriate until at least 12 months after final NCPC or Personnel Security Appeals Board action.



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

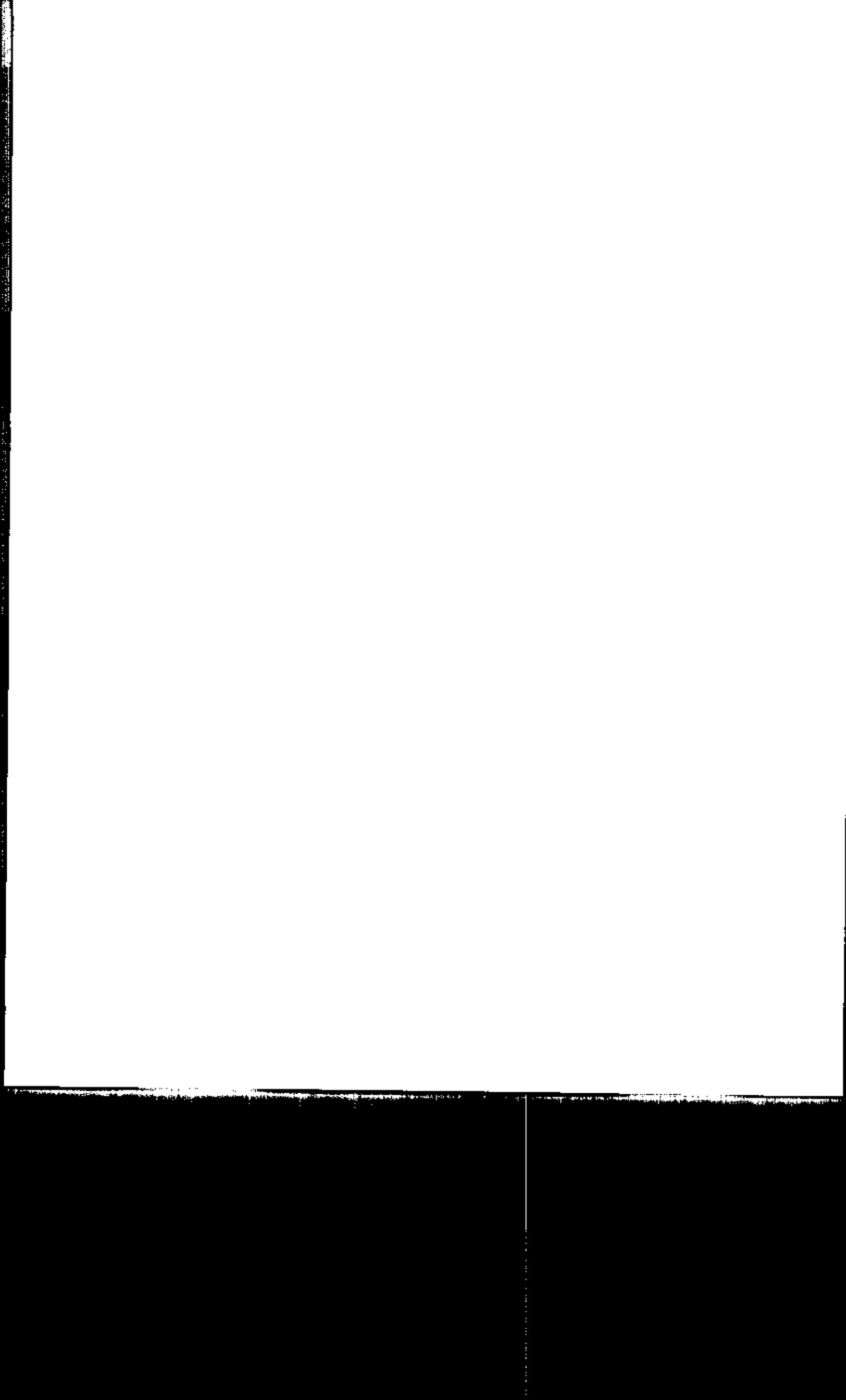
CHAPTER 24

ACCESS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	24000	24-3
REQUESTING ACCESS	24001	24-3
LOCAL RECORDS CHECK	24002	24-4
ACCESS LETTERS.	24003	24-5
ACCESS ROSTERS.	24004	24-5
TERMINATION OF ACCESS	24005	24-5
RECORDING ACCESS.	24006	24-5
TEMPORARY OR ONE TIME ACCESS.	24007	24-6
ACCESS BY INVESTIGATIVE AND LAW ENFORCEMENT AGENTS.	24008	24-6

FIGURE

24-1	REQUEST FOR ACCESS TO CLASSIFIED INFORMATION. .	24-7
24-2	FORMAT FOR LOCAL RECORDS CHECK.	24-11
24-3	FORMAT OF AN ACCESS LETTER.	24-12
24-4	SECURITY BRIEFING ACKNOWLEDGEMENT	24-13



SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

CHAPTER 24

ACCESS

24000. BASIC POLICY

1. Knowledge or possession of classified information is permitted only for individuals whose official duties require access in the interest of promoting national security and only if they have been determined to be eligible for access.
2. No individual has a right to have access to classified information solely because of grade, position or security clearance. The final responsibility for determining whether a person's official duties require access to any element or item of classified information (the "need to know"), and whether that person has been granted the appropriate security clearance by proper authority, rests upon the individual who has the authorized possession, knowledge or control of the information involved and not upon the prospective recipient.
3. These principles are equally applicable if the prospective recipient is an organizational entity, including commands, other Federal agencies, defense contractors, foreign governments and others.
4. The CO HQSVCBn, in consonance with the MARFORPAC Security Manager, will ensure that all personnel assigned to this headquarters are briefed per chapter 3 of this Manual before they are granted access to classified material.

24001. REQUESTING ACCESS

1. Division and separate branch heads will provide all requests for access to the Security Manager (AC/S G-1) (to include a request for a local records check) using the format contained in figure 24-1 of this chapter. Requests for access will be provided on an individual basis, (i.e., one person per request). The Security Manager will validate and process the request for access via the CO HQSVCBn. Once clearance has been verified and a local records check has been completed, the Security Manager will prepare and forward the access authorization letter to the appropriate section.
2. Requests for special access to the following programs will be provided as follows:
 - a. Critical Nuclear Weapons Design Information (CNWDI). Requests for CNWDI access will be provided to the Security Manager

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

via the AC/S G-2/CIHO. Prior to granting CNWDI access, personnel will be briefed and are required to sign a CNWDI briefing statement administered by the Security Manager. Access to CNWDI may be granted only to the level of final clearance.

b. Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI). Requests for SIOP-ESI access, to include the category of access required, will be provided to the Security Manager via the AC/S G-2/CIHO who will validate the requirement for access. If no valid requirement exists, the request will be returned with appropriate comments. Prior to being granted SIOP-ESI access, personnel will be briefed and required to sign a SIOP-ESI briefing statement given by the Security Manager. Requests for SIOP-ESI access should not be provided unless the individual and spouse are U.S. citizens.

c. Sealed Authentication System (SAS)

(1) Security Manager. Requests for SAS access will be provided to the Security Manager via the AC/S G-3. Upon receipt of the letter of request, the Security Manager will initiate Personnel Reliability Program (PRP) screening on the individual per the current edition of MCO 5510.7, and ~~chapter 25 of this Manual~~. If the individual does not meet the security clearance and investigative criteria for SAS access (i.e., final Top Secret clearance based on a favorably completed BI), the Security Manager will return the request to the AC/S G-3 until such time as security clearance and investigative requirements have been met. Upon successful completion of PRP screening, the Security Manager will issue a letter authorizing SAS access.

(2) AC/S G-3. If, upon receipt of the letter of request for SAS access the AC/S G-3 determines the request is inconsistent with operational requirements or should otherwise not be granted, the AC/S G-3 will immediately inform the Security Manager, in writing, of the reasons for disapproval. The Security Manager will discontinue further screening action and will notify the requester, in writing, of the disapproval.

d. North Atlantic Treaty Organization (NATO). Requests for NATO access will be provided to the Security Manager. Prior to granting NATO access, personnel will be briefed and required to sign a NATO briefing statement given by the Security Manager. Access to NATO may be granted only to the level of final clearance.

24002. LOCAL RECORDS CHECK. When divisions and separate branch heads provide a request for access, they will also include a request for a Local Records Check (figure 24-2). A Local Records Check will be conducted on all individuals by CI personnel prior to

them being granted access to classified information. The request for a Local Records Check will be provided as an enclosure to the request for access.

24003. ACCESS LETTERS. The original letter of access (figure 24-3) will be forwarded to the division/separate branch which requested access. A copy of each letter will be retained by the Security Manager. Letters of access which are sent to and maintained in division/separate branch files will serve as verification of access when requesting receipt and draw authority. These letters will be retained in the SCP custodian's turn-over folder as long as the individual is a member of the division or separate branch. The Security Briefing Acknowledgement (figure 24-4) will be completed and returned to the Security Manager.

24004. ACCESS ROSTERS. All divisions and separate branches will maintain a copy of the MARFORPAC computerized clearance and access roster. This roster is produced on a monthly basis and will be used to verify clearance and access within this headquarters. Administrative chiefs should review the roster on a monthly basis to ensure that all information is correct concerning individuals assigned within their sections.

24005. TERMINATION OF ACCESS

1. The Security Manager will be notified when an individual is transferred within this headquarters and access will be terminated accordingly. Another request for access will be provided by the gaining staff section. Administrative termination of access is not an adverse personnel security action.

2. The CO HQSVCBn may decide to restrict or suspend access on an individual when questionable or unfavorable information develops. The restriction or suspension of access for cause may only be used as a temporary measure until the individual's eligibility for access has been resolved. Upon completion of the required actions, the access must be reinstated or an adverse personnel security action must be taken per paragraph 23007 of this Manual.

24006. RECORDING ACCESS

1. The access granted must be recorded in the MMS. Access entries will be approved by the CO HQSVCBn or a designated representative. The access will be adjusted as required and the MMS will be updated as necessary to reflect current need. A record is required for the level of classification for which there is a need to know, and for

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

programs which require that access be formally granted (SIOP-ESI, NATO, CNWDI, SCI). The CO HQSVCBn will ensure that a unit diary entry is recorded for all access changes.

2. The CO HQSVCBn will ensure that the Classified Information Nondisclosure Agreement (SF 312) is completed and an appropriate entry is made in the SRB/OQR for Marine personnel and in the comments section of OPNAV Form 5520/20 for Navy personnel and civilian personnel.

24007. TEMPORARY OR ONE TIME ACCESS. The Security Manager is the only individual that can authorize emergency access to classified information within this headquarters. The procedures outlined in paragraphs 24-5 and 24-6 of OPNAVINST 5510.1H provide additional guidance on this subject.

24008. ACCESS BY INVESTIGATIVE AND LAW ENFORCEMENT AGENTS

1. Normally, investigative agents of other departments or agencies may obtain access to classified information through established liaison or investigative channels. The Security Manager will be advised on all requests for access to classified information by investigative personnel.

2. When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA) or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA or Secret Service agents may obtain access to classified information as required. However, this information will be protected as required by its classification.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5521
01
Date

From:
To: Security Manager (AC/S G-1)
Subj: REQUEST FOR ACCESS TO CLASSIFIED INFORMATION
Ref: (a) OPNAVINST 5510.1H
(b) MARFORPACO P5510.18
Encl: (1) Local Records Check Form

1. Per references (a) and (b), it is requested that the following named individual be granted access to classified information as specified:

<u>NAME</u>	<u>GRADE</u>	<u>SSN</u>	<u>ACCESS</u>
-------------	--------------	------------	---------------

SIGNATURE

Date

FIRST ENDORSEMENT

From: Security Manager (AC/S G-1)
To: Commanding Officer, Headquarters and Service Battalion,
Marine Forces Pacific
Subj: REQUEST FOR ACCESS TO CLASSIFIED INFORMATION

1. The subject request is validated. It is requested that you provide this office with the current clearance data on the individual identified.

SIGNATURE
By direction

Figure 24-1.--Request for Access to Classified Information

24-7

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

(Date)

SECOND ENDORSEMENT

From: Commanding Officer, Headquarters and Service Battalion,
Marine Forces Pacific

To: Security Manager (AC/S G-1)

Subj: REQUEST FOR ACCESS TO CLASSIFIED INFORMATION

1. Review of personnel records revealed the following clearance data:

2. The following clearance/investigative action has been taken/initiated:

SIGNATURE
By direction

Figure 24-1.--Request for Access to Classified
Information..Continued

24-8

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

1. NAME Last Name in all CAPS. Omit commas, hyphens, periods, apostrophes or blanks within the name.
Examples: DE LA MADRID = DELAMADRID; O'BRIEN = OBRLEN
JONES-SMITH = JONESSMITH
2. SOCIAL SECURITY NUMBER Self-explanatory.
3. GRADE Self-explanatory.
4. STATUS Use one of the following codes:

B - Active Duty Enlisted	L - General/Flag Officer
C - Active Duty Officer	R - Civilian Temporary/Seasonal
D - Reserve Enlisted	T - Retired General/Flag Officer
E - Reserve Officer	5 - Warrant Officer Active
S - Civilian Employee	6 - Warrant Officer Reserve
5. FORMER/MAIDEN NAMES/ALIASES If no other names enter "none".
6. DATE OF BIRTH Last two digits of the year, month, and day throughout this form.
7. PLACE OF BIRTH Enter state and county if US born; city and country if foreign born; specify part of country if politically divided (e.g., North or South Korea).
8. RETURN RESULTS TO Self-explanatory.
9. CITIZENSHIP HQSVCM Personnel Branch will verify citizenship before granting interim clearance and/or granting final clearance. Add other country in remarks for dual citizenship; certificate number and date of entry into US for naturalized citizen; or unknown.
10. ACTION REQUESTED REGARDING SUBJECT Check appropriate block.
11. SPECIAL ACCESSSES REQUESTED As required.
12. JUSTIFICATION Branch/Division heads will justify the need for clearance on personnel listed in block 1.
13. LOCAL RECORDS CHECK CERTIFICATION HQSVCM will certify completion of checks of local personnel, legal, medical, military police, security and other command records about the subject as noted. Supporting unfavorable information should be entered into remarks and/or attached.
14. CONTINUOUS FEDERAL SERVICE CERTIFICATION Enter date federal service commenced without a break of more than 24 months.
15. INTERIM CLEARANCE GRANTED Enter level of interim clearance granted, investigative basis and date interim will expire.
16. REMARKS/ENCLOSURES Use to elaborate on other information. Prior investigations will be cited by type, date completed and agency (e.g., TS/SBI/881203/DIS)
17. thru 19 Battalion Commanding Officer will sign.

Figure 24-1.--Request for Access to Classified
Information..Continued

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

LOCAL RECORDS CHECK

NAME: (Last, First, MI)

SSN:

GRADE:

MOS:

BRANCH/DIVISION:

RTD:

PREVIOUS COMMAND/MARFORPAC STAFF SECTION:

DOB:

POB:

CITIZENSHIP:

REMARKS:

(For Security Manager's Use)

SRB/OQR:

MED/DENT:

LEGAL:

DRUG/ALCOHOL:

PMO/CID:

Figure 24-2.--Format for Local Records Check.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

SECURITY BRIEFING ACKNOWLEDGEMENT

I have been briefed and fully understand my responsibilities for the security of classified information to which I am granted access. I understand that I am not to have possession or knowledge of any classified material to which I do not have a "need to know" nor am I to divulge classified information to others who do not have access or a valid "need to know." I am aware that violations of these principles or existing security regulations could result in the denial or revocation for cause of my security clearance and/or prosecution under Title 18, U.S. Code, the provisions of which I have read.

(DATE)

(SIGNATURE)

Figure 24-4.--Security Briefing Acknowledgement.

SOP FOR THE INFORMATION AND
PERSONNEL SECURITY PROGRAM

5521
01
Date

From: Security Manager (AC/S G-1)
To:
Subj: ACCESS TO CLASSIFIED MATERIAL; CASE OF
Ref: (a) OPNAVINST 5510.IH
(b) MARFORPACO P5510.18
Encl: (1) Security Briefing Acknowledgement

1. Per references (a) and (b), subject named individual is hereby authorized access to _____ material while a member of Headquarters, Marine Forces Pacific in the performance of duties with _____. Access to this sensitive information is authorized on a strict need-to-know basis.
2. Request subject named individual be briefed on the MARFORPAC control and handling procedures set forth in reference (b).
3. Subject named individual is scheduled to attend the security orientation and indoctrination brief on _____, in the H&SBn S-3 classroom. This brief is conducted in conjunction with the Command Orientation Briefing.
4. Request enclosure (1) be completed and returned to the Security Manager (AC/S G-1).
5. All previous access authorizations granted for subject named individual are void.

SIGNATURE
By direction

Copy to:
PersO/Unit Diary

Figure 24-3.--Format of an Access Letter.