



# UNITED STATES MARINE CORPS

MARINE CORPS BASE HAWAII  
BOX 63002  
MCBH KANEOHE BAY, HI 96863-3002

IN REPLY REFER TO:  
BaseO P5511.3  
G-1

20 MAY 2003

## BASE ORDER P5511.3

From: Commanding General  
To: Distribution List

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

Ref: (a) SECNAVINST 5510.30A  
(b) SECNAVINST 5510.36  
(c) MCO P5510.18A w/ CH1  
(d) BaseO P2280.1  
(e) USCINCPAC OPORD 5050-99  
(f) SECNAVINST 5239.3  
(g) MCO 5215.1H

Encl: (1) Locator Sheet

1. Purpose. To publish the policies and procedures for Marine Corps Base Hawaii's (MCBH) Information and Personnel Security Program (IPSP) in accordance with the references.

2. Cancellation. BaseO P5511.2.

3. Recommendations. Recommendations concerning the contents of the Manual are invited and should be submitted to the Base Security Manager.

4. Certification. Reviewed and approved this date.

A handwritten signature in black ink, appearing to read "R. C. Roten".

R. C. ROTEN  
Deputy Commander

DISTRIBUTION: B

LOCATOR SHEET

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

Location: \_\_\_\_\_  
(Indicate the location(s) of the copy(ies) of this Manual.)

SOP FOR IPSP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature

SOP FOR IPSP

CONTENTS

CHAPTER

	INTRODUCTION
1	BASIC POLICY AND APPLICABILITY
2	SECURITY PROGRAM MANAGEMENT
3	PERSONNEL SECURITY
4	INFORMATION SECURITY
5	COMMUNICATIONS SECURITY
6	SECURITY EDUCATION AND TRAINING
7	SECURITY VIOLATIONS AND INVESTIGATIONS

## SOP FOR IPSP

### INTRODUCTION

0001. PURPOSE. To promulgate the policies and procedures for the administration of the Base Information and Personnel Security Program (IPSP).

0002. STATUS

1. Requirements in this Manual are binding on all Base personnel.
2. Any deviation from instructions contained in this Manual must be authorized by the Commanding General, Marine Corps Base Hawaii, Kaneohe Bay.

0003. SCOPE. This Manual contains guidelines and basic procedures for the control and protection of classified information. This Manual specifies what must be done, who is to do it, and who is to supervise it.

0004. RESPONSIBILITY. The currency, accuracy, modification and distribution of this Manual are the responsibility of the base security manager.

0005. CHANGES. Changes will be made to this Manual in accordance with instructions contained in the current edition of reference (g). Such changes will be numbered consecutively and entered accordingly on the Record of Changes, page (i), provided for that purpose.

SOP FOR IPSP

CHAPTER 1

BASIC POLICY AND APPLICABILITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
POLICY	1000	1-1
APPLICABILITY	1001	1-1

## SOP FOR IPSP

### CHAPTER 1

#### BASIC POLICY AND APPLICABILITY

1000. POLICY. The IPSP is designed to protect essential national security information. The program is based on the following precepts:

1. Limitation of Classified Material Holding. Classified Material must be held to a manageable level by avoiding improper or over classification, downgrading or declassifying information which requires a lesser degree of protection and destruction of classified matter no longer required.
2. Safeguarding of Classified Material. Classified material will be protected against unauthorized disclosure during storage, use, transmission, distribution, and destruction.
3. Control of Dissemination. Prior to the release of classified information, the individual having control of that information will determine that the intended recipient has an appropriate clearance, has been granted access to the level of information requested, and has an official need to know.
4. Report of Violation. Violations of security regulations are serious offenses and must be reported immediately to the commanding general via the security manager. All incidents involving disciplinary action taken on personnel who possess a security clearance must be reported to the Security Manager.

1001. APPLICABILITY. The provisions of the current edition of references (a) through (g) and this Manual are applicable to all military and civilian members of this command.

SOP FOR IPSP

CHAPTER 2

SECURITY PROGRAM MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	2000	2-1
PERSONNEL	2001	2-1
PROCEDURES	2002	2-2
FACILITIES	2003	2-2

## SOP FOR IPSP

### CHAPTER 2

#### PROGRAM MANAGEMENT

2000. GENERAL. The IPSP is a system of personnel, procedures, and facilities. The structure of this system is described in the following paragraphs.

2001. PERSONNEL. All personnel who handle classified material within this command will be thoroughly familiar with the current edition of reference (b).

1. Commanding General. The commanding general is responsible for security of classified information within this command and for instruction of personnel in security practices and procedures.

2. Security Manager. The security manager must be a U.S. citizen, an officer or civilian employee (GS-11 or above), satisfactorily complete a background investigation, be granted a final TOP SECRET clearance, and be designated by letter of appointment. The security manager will oversee the management of the Base IPSP and advise the commanding general in all matters pertaining to personnel security and the security of classified information.

3. Assistant Security Manager. The Assistant Security Manager must be a U. S. citizen, an enlisted person (E-6 or above), or civilian (GS-6 or above). The assistant must satisfactorily complete a background investigation, be granted a final TOP SECRET clearance, and be designated by letter of appointment. Under the supervision of the Security Manager, the Assistant Security Manager will assist in the day-to-day management of the security program.

4. Top Secret Control Officer (TSCO). The TSCO must be an officer, enlisted person (E-7 or above), or civilian (GS-7 or above). The TSCO must satisfactorily complete a background investigation, be granted a final TOP SECRET clearance, and shall be designated by letter of appointment. The TSCO is responsible for and reports to the security manager regarding the receipt, custody, accountability and disposition of TOP SECRET material.

5. Officer-in-Charge, Classified Material Control Center (OIC, CMCC). The OIC, CMCC, must satisfactorily complete a background investigation, be granted a final TOP SECRET clearance, and shall be assigned by letter of appointment. The OIC, CMCC is responsible for security and accountability of classified material.

## SOP FOR IPSP

6. Secondary Control Point Officer (SCPO). The SCPO must be an officer, enlisted person (E-7 or above ), or civilian (GS-7 or above). The TSCO must satisfactorily complete a background investigation, be granted a final SECRET clearance, and shall be designated by letter of appointment. Under the supervision of the OIC, CMCC, the SCPO will safeguard and account for classified material held by the SCP.

7. Information System Security Manager (ISSM). The ISSM is responsible for development, maintenance, and implementation of the information security (INFOSEC) program. The ISSM serves as the command's point of contact for INFOSEC issues and coordinates with the Security Manager in the day-to-day management of the INFOSEC program. The ISSM shall be designated by letter of appointment.

8. Communications Security Material System (CMS) Custodian. The CMS custodian must be an officer or an enlisted person (E-7 or above), who has satisfactorily completed a Background Investigation and been granted a final TOP SECRET clearance. This person shall be designated by letter of appointment and will be thoroughly familiar with the current edition of reference (d).

9. Subordinate units. The Commanding Officers, Headquarters Battalion (CO, HQBN) and Marine Corps Air Facility (CO, MCAF), shall assist the Security Manager in those aspects of the IPSP relating to security education and the granting and termination of access.

2002. PROCEDURES. The basic procedures to be followed by personnel designated to function within the Base IPSP management structure are contained in the current edition of reference (b) and this Manual.

2003. FACILITIES. Classified material must be stored or used in facilities or under conditions adequate to prevent unauthorized persons from granting access to it. Classified material storage and control facilities will be established only after they have been authorized in writing by the Security Manager.

1. Classified Material Control Center (CMCC). A CMCC will be established as the command level facility for receipt, handling, control, storage, dissemination, and disposal of classified material originated or reviewed by the command. Written desktop procedures which will cover all phases of the internal operation of the CMCC will be promulgated. The Base CMCC is located in building 216.

2. Secondary Control Point (SCP)

a. A SCP is a designated classified material storage area. The SCP custodian draws classified material from the CMCC for retention. The three SCPs that fall under the purview of the MCBH Security

SOP FOR IPSP

Manager are the ACS/G-3, Marine Corps Air Facility, and Explosive Ordnance Disposal.

b. To establish an SCP, a written request containing the following information shall be forwarded to the Security Manager.

(1) The desired location of the SCP.

(2) The volume and highest classification of classified material to be retained.

(3) In cases where only SECRET and CONFIDENTIAL materials are handled, waivers of rank requirements may be granted by subordinate commanders if the requirements of intelligence, reliability, and demonstrated maturity are fulfilled in appointing a person of lesser grade.

(4) A request that a site evaluation for the proposed SCP be conducted.

c. The Security Manager will accomplish the following upon receipt of the request:

(1) Request a site evaluation be conducted by the Physical Security Branch of the Provost Marshal's office.

(2) Provide written approval or disapproval for the establishment of the control point, to include the volume and highest classification of material authorized for storage.

(3) If approved, a copy of the appointment letter for control point officials and certification of their clearance and access will be provided to the CMCC.

3. Disestablishment of SCP. When the requirement for a control point no longer exists, the following action will be taken:

a. Notify the Security Manager in writing of the intent to disestablish the control point and provide him with the anticipated date of final action. A copy of the notification will be provided to the CMCC. If the Security Manager disagrees with the intent to disestablish, he will immediately take steps to resolve the matter with the cognizant official.

b. Conduct an inventory of all classified material held by the control point and resolve any discrepancies with the CMCC.

## SOP FOR IPSP

c. Review all classified material held to determine the need for retention. Material to be destroyed will be listed on both the inventory report and on a Classified Material Destruction Report that may be obtained from the CMCC.

d. Once disestablishment is approved, return all classified material to the CMCC. The CMCC will review the inventory for accuracy, sign for the material received, and destroy all material on the Classified Material Destruction Report.

e. The custodian will conduct a thorough inspection of the vacated site to ensure the absence of classified material. The results will be communicated to the CMCC custodian.

SOP FOR IPSP

CHAPTER 3

PERSONNEL SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
ELIGIBILITY AND ACCESS	3000	3-1
DENIAL OR SUSPENSION OF CLEARANCE FOR CAUSE	3001	3-2
SPECIAL ACCESS PROGRAMS	3002	3-2
VISITOR CONTROL	3003	3-2
FOREIGN TRAVEL	3004	3-4

SOP FOR IPSP

CHAPTER 3

PERSONNEL SECURITY

3000. ELIGIBILITY AND ACCESS

1. Basic Policy

a. Eligibility for access to classified information or assignment to sensitive duties shall be based on a command determination of a member's loyalty, reliability, trustworthiness and satisfactory completion of a personnel security investigation appropriate to the level of access required. It is imperative that access be kept on a strict need-to-know basis and that the number of personnel with access be kept to the minimum required to ensure mission accomplishment.

b. No member of this command will be granted access to classified information or be assigned to sensitive duties unless such assignment is clearly consistent with the interests of national security and essential to mission accomplishment.

2. Request for Personnel Security Investigation (PSI)

a. Requests for PSIs will be submitted in writing to the Security Manager. A justification letter is required stating specifically why the clearance is needed and what level of access is required.

b. The Security Manager is authorized to grant an Interim Confidential, Interim Secret, or Interim Top Secret clearance and will approve or disapprove the request for access to classified information based on the following:

(1) A properly completed Electronic Personnel Security Questionnaire that contains no disqualifying information.

(2) A properly completed Local Records Check that includes a check of personnel records.

(3) A favorable National Agency Check (required for Interim Top Secret only).

c. Final clearance determination is made by the Department of the Navy Central Adjudication Facility after submission of all personnel security documents.

## SOP FOR IPSP

3. Termination of Access. Access to classified information will automatically be terminated when an individual transfers from the command, is discharged or separated, or when a security clearance is withdrawn, denied, or suspended for cause. Upon termination of access, the individual must report to the security office for a debriefing.

3001. DENIAL OR SUSPENSION OF CLEARANCE FOR CAUSE. When a personnel security determination has been made that an individual does not meet or no longer meets the criteria contained in reference (a), their access to classified material will be denied or suspended for cause by the Security Manager. If questionable or unfavorable information becomes available on an individual who has been granted access, the Security Manager may restrict or suspend their access as a temporary measure until the individual's eligibility for continued access has been determined.

3002. SPECIAL ACCESS PROGRAMS. Definition: Any program requiring additional security protection and handling measures, or special investigative, adjudicative, and clearance procedures or special access. The CMCC currently has three special access programs: Personnel Reliability Program, Critical Nuclear Weapons Design Information, and the North Atlantic Treaty Organization.

1. Personnel Reliability Program (PRP). The PRP restricts access to nuclear weapons through controlled and critical billets. The Explosive Ordnance Disposal (EOD) Officer will assume the duties of the PRP Officer.

2. Critical Nuclear Weapons Design Information (CNWDI). CNWDI access is normally limited to EOD personnel, however, other personnel may qualify on a need-to-know basis. The EOD Officer will screen all EOD personnel and their records for eligibility for access to CNWDI material and will provide initial briefings and refresher training. Personnel must be debriefed when access to CNWDI is terminated. Individual briefing/debriefing records will be maintained for two years from the date of termination.

3. North Atlantic Treaty Organization (NATO). All personnel with access to NATO classified information will be briefed on its sensitivity. A file copy of the briefing and debriefing statements will be retained by the CMCC for one year from the date of termination.

3003. VISITOR CONTROL

1. Visitor. Any person who is not a military member or civilian employee of this command.

## SOP FOR IPSP

2. Visit. A visit is made when the visitor enters any area under the jurisdiction of the Commanding General, Marine Corps Base Hawaii.

a. General Visit. A general visit is one made to this command by U.S. Citizens or immigrant aliens for authorized personal or professional purposes. All general visits will be on an unclassified basis and no classified information or area will be divulged or shown.

b. Controlled Visit. A controlled visit is one made to this command by any visitor during which classified information may be discussed or a classified area visited.

3. Visitor Control Procedure. Visitor control procedures are outlined in reference (a) and will be strictly adhered to.

4. Processing of Visit Request. The Security Manager will receive and process all requests in coordination with command element(s) to be visited. Classified visits will be processed in accordance with reference (a). A copy of the request will be maintained by the Security Manager.

### 5. Visitor Handling

a. Visitors, whose requests have been approved, will be escorted by a representative of the command element being visited. The escort will ensure that the scope of the visit is limited to material and classification levels authorized in the request.

b. Visitors, whose requests have not been received or who hand carry their visit request, will be escorted to the Security Manager, who will attempt to verify the validity/legitimacy of the visit.

c. Visitors to the CMCC/SCPs will be required to log in and out.

6. Visit Request for Command Member. When members of this command are required to conduct visits or attend meetings at which classified information will be discussed, the Security Manager will send the necessary visit request. It is imperative that personnel who require visit requests notify the Security Manager as soon as possible so that the visit request can be transmitted in a timely manner. It is also recommended that personnel contact the destination location prior to travel to confirm receipt of the visit request.

7. Foreign Visitors. Official visits to Marine Corps Base Hawaii by representatives of foreign governments must be approved by the Navy International Programs Office or an authority specifically designated in reference (a) regardless of whether classified information will be disclosed. The Command Security Manager at Camp Smith is the primary point of contact for foreign visits throughout MARFORPAC.

SOP FOR IPSP

3004. Foreign Travel. Per reference (e), all personnel deploying or traveling to countries in the U.S. Pacific Command area of responsibility that are not U.S. territories or possessions must comply with Anti-Terrorism/Force Protection (AT/FP) requirements prior to departure. Specific AT/FP requirements vary by country and are constantly changing; therefore, personnel are advised to contact their unit AT/FP officer for guidance.

SOP FOR IPSP

CHAPTER 4

INFORMATION SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
INFORMATION SYSTEMS SECURITY	4000	4-1
CONTROL AND DISSEMINATION	4001	4-2
RESPONSIBILITY OF CUSTODIANS	4002	4-3
CARE OF WORKING SPACES	4003	4-3
CARE DURING WORKING HOURS	4004	4-3
INVENTORIES	4005	4-4
INSPECTIONS	4006	4-4
STORAGE CONTAINERS	4007	4-4
COMBINATIONS	4008	4-5
SECURITY CHECKS	4009	4-5
TRANSPORTATION	4010	4-5
REPRODUCTION	4011	4-6
ROUTINE DESTRUCTION OF CLASSIFIED	4012	4-6
EMERGENCY ACTION PLAN	4013	4-7
CLASSIFICATION MANAGEMENT	4014	4-7
CLASSIFIED MEETINGS	4015	4-7
DISCLOSURE TO THE PUBLIC	4016	4-8

SOP FOR IPSP

CHAPTER 4

INFORMATION SECURITY

4000. INFORMATION SYSTEMS SECURITY

1. Information systems security is comprised of two key areas, Information Assurance and Computer Security. Information Assurance (IA) is defined as the protection of information systems against:

- a. Unauthorized access to or modification of information.
- b. Denial of service to authorized users.
- c. Providing service to unauthorized users.

2. IA also includes the measures taken to detect, document, and counter these threats.

3. Computer Security is defined as the protection of hardware and software containing classified information against unauthorized use and/or disclosure. The following guidelines are to be strictly adhered to in processing classified information on any information system (IS):

a. Information can only be processed, stored, or transmitted on a system/network that meets the requirements for classified processing. This information will not exceed the approved classification level for the system/network.

b. All IS will utilize some form of access control to ensure only authorized personnel have access.

c. Network systems will meet required encryption and cabling requirements. Servers will be located in a vault/secure room authorized for open storage at the level of the server.

d. Workstations and stand-alone systems will either have removable hard drives or be located in a vault/storage room authorized for open storage at the level of the system utilized.

e. All computer hardware and software used to process classified must be labeled or marked at the highest level of classification utilized.

4. The Assistant Chief of Staff (ACS), G-6, has overall responsibility for information systems security and will advise and assist the Security Manager in those areas that specifically involve

## SOP FOR IPSP

classified information. Specifically, the Security Manager will coordinate with G-6 representatives on:

a. Personnel security - ensuring that personnel with access to classified information systems have the requisite clearance to operate those systems.

b. Physical security - protection of classified information systems from damage, loss, theft or unauthorized access.

c. Procedural security - ensuring continuous operation of classified information systems. "Spillages", or other information system-related security violations will be reported immediately to the Security Manager. Copies of follow-up incident reports will be forwarded to the Security Manager.

d. Training - ensuring personnel with access to classified information systems receive regular training on proper usage of such systems.

5. The ACS, G-6 will ensure the following security personnel are designated in writing:

a. Information Systems Security Manager (ISSM) - The ISSM serves as the command's point of contact for all IA issues.

b. Information Systems Security Officer (ISSO) - The ISSO serves as the command's point of contact for each information system and maintains IS security requirements.

c. Network Security Officer (NSO) - The NSO serves as the command's point of contact for each network and maintains network security requirements.

6. Reference (f) provides more detailed guidance on Information Systems Security.

4001. CONTROL AND DISSEMINATION. The following procedures provide guidance for the accounting and control of each level of classified material handled by the command.

1. TOP SECRET. The Top Secret Control Officer is primarily responsible for receipt, maintenance, and destruction of TOP SECRET material. TOP SECRET information originated or received by the command will be continuously accounted for, individually serialized, and entered into a command TOP SECRET log. The log will completely identify the information to include the date originated or received, a serial number, copy number, title, number of pages, and disposition (transferred, destroyed, transmitted, downgraded, declassified, etc.)

## SOP FOR IPSP

2. SECRET and CONFIDENTIAL. SECRET and CONFIDENTIAL information originated or received by the command will be controlled using procedures that are commensurate with the command's location, mission, local environment, and assessment of the threat.

3. WORKING PAPERS. Working papers are not considered finished documents and can include such things as drafts and classified notes taken during training. Working papers shall be:

- a. Dated when created.
- b. Conspicuously marked "Working Papers" on the first page in letters larger than the text.
- c. Marked in the center of the top and bottom of each page with the highest overall classification of the information.
- d. Protected according to assigned classification level.
- e. Destroyed by authorized means when no longer needed.
- f. Controlled as a finished document if retained or released outside the command more than 180 days after creation.

4002. RESPONSIBILITY OF CUSTODIANS. Classified material will be stored or used only in facilities or under conditions adequate to prevent unauthorized access. Custodians of classified material are responsible for safeguarding it at all times and securing the material when it is not in use or under the direct supervision of authorized personnel. Custodians will ensure that unauthorized persons do not gain access to classified information by sight, sound, or other means.

4003. CARE OF WORKING SPACES. In order to prevent unauthorized access, buildings and spaces used for storage and processing of classified information must be afforded protective security measures commensurate with the highest level of information used in these facilities. Reference (a) contains the specific physical security measures required for Confidential, Secret, and Top Secret material.

4004. CARE DURING WORKING HOURS. Precautions must always be taken to prevent unauthorized disclosure of classified information. Members of this command who are using classified material during working hours:

1. Will keep classified material in a security folder with the proper cover sheet.
2. Will keep classified material under direct control or surveillance.

## SOP FOR IPSP

3. Will return classified material to the CMCC or SCP when no longer being used and definitely by the end of the working hours.

4. Will use a secure telephone when discussing classified information.

5. Will not intermingle classified material with unclassified material. In areas that lack authorization for open storage, distinctly colored or labeled in-boxes will be used to temporarily hold classified material and keep it separate from unclassified information. These boxes will be turned upside down when securing for the day to indicate no classified remains in the work area.

4005. INVENTORIES. An inventory of all classified material held by control points will be conducted as follows:

1. Upon relief of a custodian or alternate custodian.
2. When security containers are found open and a possible compromise has occurred.
3. When any member with access to the CMCC or a SCP commits suicide, attempts to commit suicide, or is in an unauthorized absence status for 48 hours or more, a complete inventory will be conducted.

4006. INSPECTIONS. The Security Manager will conduct an annual inspection of all SCPs. The purpose of these inspections is to ensure compliance with command security procedures and to identify weaknesses in control point security procedures. An inspection checklist will be provided to all SCPs prior to inspection. The Security Manager will also periodically conduct random, unannounced inspections of the CMCC and SCPs during and after working hours. Security violations and practices dangerous to security will be noted and reported for appropriate action.

4007. STORAGE CONTAINERS. Only GSA-approved security containers will be used for storing classified material and only GSA-approved containers will be procured when new storage equipment is required. GSA-approved equipment will normally have a plate affixed to the equipment indicating it is certified for the storage of classified information. This plate will not be removed, painted over, or otherwise rendered unreadable. In addition, security containers will not have any external markings that indicate the level of classified material stored within. Each storage container for classified material will have the following:

1. A recall card indicating the individual and alternates responsible for the contents of the container, their home address and telephone numbers.

## SOP FOR IPSP

2. A Safe Log, such as the Standard Form 702, will be used to document the time and date of each opening and closing of the container.
3. An "Open" and "Closed" sign will be used on all containers and will be appropriately displayed indicating the safe's condition at any given time.

### 4008. COMBINATIONS

1. Combinations will be changed under any of the following conditions: every two years, upon change of custodian, upon compromise or subjection to compromise, or when an individual with knowledge of the combination is transferred.
2. Only personnel with the appropriate clearance, access, and a need-to-know will hold the combination to a safe or security container.
3. A record of all combinations to the CMCC will be delivered to the Communications Center for storage. The combinations will be sealed in an envelope and will contain the names and signatures of all personnel authorized access to the combinations. In the event of an emergency, these combinations may be released to the authorized individuals and, in their absence, the CDO.
4. The combinations to a safe or security container will be classified at the same level as the material stored within the safe and will be afforded the same level of protection.
5. Combinations to classified storage containers of all SCPs will be held by the CMCC. SCPOs will ensure combinations are changed as stated in subparagraph 4008 (1).

4009. SECURITY CHECKS. A Standard Form 701 will be used to secure rooms or vaults where classified material is used. This form is normally affixed to the main door to ensure end-of-day safety and security checks are conducted and that all classified material is properly secured.

4010. TRANSPORTATION. The term "transportation" refers to any physical movement of classified information from one place to another. Classified information will be transported either in the custody of any appropriately cleared individual or by an approved system or carrier, as per reference (b). All personnel who plan to transport classified material from this command will first coordinate with the Security Manager. The Security Manager will review the material for proper wrapping and marking, ensure the proper transfer method is being used, and that the individual handling the material is properly cleared and fully aware of their responsibilities.

## SOP FOR IPSP

### 4011. REPRODUCTION

1. Authorization Officials. Classified documents will be reproduced only to the extent required by operational necessity. Copiers used to reproduce classified will be located in easily observable areas. Personnel making copies of classified information will ensure that:

a. Copies are only made on machines authorized for classified reproduction (a sign indicating such authorization should be located near the copier).

b. Copies are afforded the same level of protection as original documents.

c. Reproduction limitations placed by originators of the documents are adhered to.

d. A thorough check of the copier is conducted to ensure no classified remains in the area and that any classified waste is properly destroyed.

e. Two or more blank copies are run through the copier to ensure no latent images of classified material remain.

4012. ROUTINE DESTRUCTION OF CLASSIFIED. The proper destruction of unneeded classified material is essential to an effective security program. It allows for better protection by minimizing classified holdings, reduces storage requirements and administrative workload, and better prepares the command in the event emergency destruction of classified material is required. Classified information will be only be destroyed by authorized means and only by personnel cleared to the level of information being destroyed. Procedures for destroying classified and the equipment used to accomplish the destruction will meet the criteria outlined in reference (b).

1. Top Secret information requires a record of destruction that fully identifies the material, shows number of copies destroyed, is signed by two cleared witnesses, and shows date of destruction. The record of destruction may be in electronic form such as a computer database.

2. Secret and Confidential information require no record of destruction except for Special Programs.

3. Burn bags may be used if classified information cannot be immediately destroyed. Burn bags should have unique markings or labeling that identify them as classified and they should not be located next to or in the immediate vicinity of unclassified trash. Once full, and until properly destroyed, burn bags will be sealed and safeguarded at the level of classified material they contain.

## SOP FOR IPSP

4013. EMERGENCY ACTION PLAN (EAP). Emergency Action Plans will be developed by each SCP for the protection, removal, and destruction of classified material. EAPs will include detailed procedures for guarding classified material, for removing it from the immediate area, and for complete destruction on a phased, priority basis. Emergency plans should be designed to provide minimal risk to the lives of personnel while ensuring the rapid removal/destruction of classified material with maximum security.

### 4014. CLASSIFICATION MANAGEMENT

1. Original Classification Authority. The Commanding General and the Deputy Commander of Marine Corps Base Hawaii have authority to originally classify information as SECRET or CONFIDENTIAL. Original classification of information generated by this command will meet the criteria established in reference (b). Determination of TOP SECRET classification, if required, will be made by the Commander, Marine Forces Pacific.

2. Derivative Classification. Information originated from this command that incorporates, paraphrases, restates, or generates in new form, information that is already classified, will derive its classification from the source material and will not require an original classification determination.

4015. CLASSIFIED MEETINGS. The potential for inadvertent disclosure of classified information is high at meetings and conferences due to the sometimes-large number of attendees. It is the responsibility of the individual sponsoring a classified meeting or conference to provide adequate security measures. The point of contact for any such meeting or conference will coordinate with the Security Manager to ensure that:

1. Areas where classified information is discussed provide adequate protection against unauthorized access.
2. Identification and security clearances of all attendees have been verified. Any attendee who does not possess the requisite clearance or whose clearance cannot be verified will be asked to leave until the classified portion is over.
3. Signs are displayed indicating the highest level of classified information to be discussed.
4. Briefers announce the classification of their briefing at the start and finish of their presentation.

SOP FOR IPSP

5. A thorough clean up is conducted after the meeting/conference to ensure any classified papers or documents have been secured. Any classified notes taken during the event are considered classified working papers and must be afforded the proper level of protection.

4016. DISCLOSURE TO THE PUBLIC. The Public Affairs Officer is tasked with informing the public to the maximum extent possible but within the confines of national security. However, this does not require or authorize the public release of classified information without specific approval of the Commanding General. Photography of classified work areas and designated restricted areas is not authorized, whether for commercial or personal purposes. Witnesses to any such photography should immediately notify the Provost Marshal's Office.

SOP FOR IPSP

CHAPTER 5

COMMUNICATIONS SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	5000	5-1
COMSEC DISCIPLINES	5001	5-1
TELEPHONE USE	5002	5-1
REFERENCES	5003	5-1

SOP FOR IPSP

CHAPTER 5

COMMUNICATIONS SECURITY

5000. GENERAL. Communications Security (COMSEC) is defined as the protective measures taken to deny unauthorized persons information derived from telecommunications related to national security and to ensure the authenticity of those telecommunications.

5001. COMSEC DISCIPLINES. COMSEC is comprised of the following components:

1. Crypto security. The component of COMSEC that results from providing technically sound cryptosystems and their proper use.
2. Physical Security. The component of COMSEC, which results from the physical measures taken to safeguard COMSEC material and information from unauthorized persons.
3. Transmission Security. The component of COMSEC which results from measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.
4. Emission Security. The component of COMSEC which results from measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of comprising emanations from crypto-equipment and telecommunications systems.

5002. TELEPHONE USE. Classified information will never be discussed on non-secure telephones. This restriction includes attempts to "talk around" classified subjects. Personnel should always be aware that even unclassified information, when combined with other intercepted communications, could reveal operational information that provides adversaries with our capabilities and intentions. When in doubt, use a secure telephone or other secure means of communication.

5003. REFERENCES. Refer to reference (d) for more in-depth guidance on COMSEC issues.

SOP FOR IPSP

CHAPTER 6

SECURITY EDUCATION AND TRAINING

	<u>PARAGRAPH</u>	<u>PAGE</u>
PURPOSE	6000	6-1
RESPONSIBILITY	6001	6-1
CLASSES/BRIEFS	6002	6-1

SOP FOR IPSP

CHAPTER 6

SECURITY EDUCATION AND TRAINING

6000. PURPOSE. The objective of security education is to develop and maintain security discipline by creating a sense of personal responsibility and security awareness in each member of the command.

6001. RESPONSIBILITY

1. The purpose of the security education program is to promote a high level of security awareness throughout the command. To accomplish this, the Security manager, in coordination with subordinate commanders, will develop and implement a security education program based on the needs of this command and the requirements of reference (a).

2. Department/section heads and chiefs will provide ongoing reinforcement of the security education program by ensuring strict adherence to security measures related to the handling of classified information.

6002. CLASSES/BRIEFS. Each command that handles classified information shall establish and maintain an active security education program to instruct all command personnel in security policies and procedures. Requests for security classes and assistance in training will be directed to the Security Manager. The Security Manager will be responsible for briefing and debriefing all personnel with access to classified information as outlined in reference (a). Minimum briefing requirements are listed below:

1. Indoctrination
2. Orientation
3. On-the-job training
4. Annual refresher
5. Counterintelligence
6. Special (example: Foreign travel)
7. Debriefing

SOP FOR IPSP

CHAPTER 7

SECURITY VIOLATIONS AND INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
SECURITY VIOLATIONS	7000	7-1
COMPROMISE OR SUBJECTION TO COMPROMISE PRELIMINARY INQUIRY	7001	7-1
JAG MANUAL INVESTIGATION	7002	7-2
MATTERS TO BE REPORTED TO THE SECURITY MANAGER	7003	7-2

## SOP FOR IPSP

### CHAPTER 7

#### SECURITY VIOLATIONS AND INVESTIGATIONS

7000. SECURITY VIOLATIONS. A security violation is any failure to comply with regulations relative to the security of classified information. All security violations will be immediately reported to the Security Manager whether or not classified information was compromised or subjected to possible compromise.

7001. COMPROMISE OR SUBJECTION TO COMPROMISE/PRELIMINARY INQUIRY. When classified information has been, or may have been, disclosed to unauthorized personnel, the Security Manager will be notified immediately. Upon notification, the Security Manager will notify the local NCIS field office. The command with custodial responsibility of the material in question will conduct a preliminary inquiry in accordance with reference (b). The preliminary inquiry will be delivered to the Security Manager and contain the following information:

1. Complete identification of all classified information involved: Classification, serial numbers, dates, originator, subject or equipment function, downgrading and declassification instructions, and number of pages per document.
2. Identification of all personnel involved by full name, grade, social security number and billet title.
3. A chronological report of events related to the incident and the time and frame during which the information was subject to compromise.
4. Results of interviews with all witnesses to the incident.
5. The person(s) responsible for the classified information subjected to compromise.
6. Identification of weaknesses in security procedures that allowed the information to be subjected to compromise.
7. The probability of compromise, stated in one of the following ways:
  - a. "Confirmed": when conclusive evidence exists that unauthorized persons gained access to the information and that identifiable damage to national security may result.

SOP FOR IPSP

b. "Cannot be discounted": when some evidence exists that unauthorized persons gained access and that identifiable damage to national security may result.

c. "Occurred, but under conditions presenting minimal risk to national security": when some evidence exists that unauthorized persons gained access to the material but there is no evidence that identifiable damage to the national security is likely to result.

d. "Did not occur": When there is not evidence that unauthorized persons obtained meaningful knowledge of the material.

8. Recommendations of actions to be taken to prevent a recurrence.

9. Recommendations as to whether disciplinary action is appropriate.

7002. JAG MANUAL INVESTIGATION. When it is determined that compromise is confirmed or cannot be discounted, that significant security weaknesses are present, or that punitive action is appropriate, a JAG Manual Investigation will be initiated as per reference (b). A summary of the preliminary inquiry's findings, endorsed to indicate that a JAG Manual Investigation should be initiated, will be delivered to the Security Manager.

1. The Security Manager will notify, or forward reports to the originator of the compromised information, Naval Criminal Investigative Service (NCIS), and higher headquarters as appropriate.

2. An officer will be appointed to conduct the investigation and will inform the Security Manager of the findings.

7003. MATTERS TO BE REPORTED TO THE SECURITY MANAGER. All members of this command will immediately report to the Security Manager any of the following:

1. Sabotage, Espionage or Deliberate Compromise. Individuals becoming aware of possible acts of sabotage, espionage, terrorism, or suspicious foreign contacts will immediately report the information to their Security Manager, Commanding Officers or the most readily available command. The command receiving the report will notify NCIS.

2. Suicide or attempted suicide. When a member of this command who has or had access to classified information commits suicide or attempts suicide, immediately notify the Security Manager who will forward the information to the local NCIS office for action.

## SOP FOR IPSP

3. Unauthorized Absentees. When a member of this command who has access to classified information is in an unauthorized absence status, the Security Manager will be notified. The Security Manager shall conduct an inquiry to determine if there are any indications that the individual's activities, behavior, or associations may have been harmful to national security. If such indications exist, the Security Manager will immediately notify the Commanding Officer and report the information to NCIS.