



UNITED STATES MARINE CORPS

MARINE CORPS AIR STATION YUMA
BOX 99100
YUMA, ARIZONA 85369-9100

StaO P5510.30B

MAD

22 JUL 2009

STATION ORDER P5510.30B

From: Commanding Officer, Marine Corps Air Station Yuma
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR MARINE CORPS AIR STATION
YUMA INFORMATION AND PERSONNEL SECURITY PROGRAM (SHORT
TITLE: IPSP)

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.30
(d) Sta(O) 2280.1
(e) MCO 5239.2
(f) Sta(O) 5510.12
(g) Sta(O) 5510.15
(h) Sta(O) 5720.6

Encl: (1) Locator sheet

1. Purpose. To establish Standing Operating Procedures for the MCAS Yuma Information and Personnel Security Program (IPSP).

2. Cancellation. StaO P5510.30A

3. Background. This directive supplements the references. It serves as policy except where it contradicts any regulation issued by a higher headquarters in which case the higher headquarters directive shall prevail in determining actions. This directive is applicable to all military, civilian, and contractor personnel assigned to MCAS Yuma.

4. Action. Commanding Officers, Department Heads, Supervisors, and Contracting Officers are responsible for the full implementation of this directive as it pertains to their organization.


M. A. WERTH

Distribution: A

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR MARINE CORPS AIR
STATION YUMA INFORMATION SECURITY PROGRAM (SHORT TITLE: IPSP)

Location:

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

Enclosure (1)

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

RECORD OF CHANGES

Log completed change action as indicated:

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CONTENTS

CHAPTER

- 1 Introduction
- 2 Command Security Management
- 3 Counterintelligence Matters
- 4 Security Education Program
- 5 National Security Positions
- 6 Personnel Security Investigations
- 7 Personnel Security Determinations
- 8 Clearances
- 9 Access to Classified Information
- 10 Continuous Evaluation
- 11 Visitor Control
- 12 Classification Management
- 13 Marking
- 14 Safeguarding
- 15 Dissemination, Transmission and Transportation
- 16 Storage and Destruction
- 17 Industrial Security Program
- 18 Loss or Compromise of Classified Information

CHAPTER 1
INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	1000	1-2
Objectives	1001	1-2
Responsibility for Compliance	1002	1-2
Policy Guidance	1003	1-2

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CHAPTER 1

INTRODUCTION

1000. Basic Policy. The MCAS Yuma IPSP is established in compliance with the Department of the Navy (DON) Information and Personnel Security Programs to ensure that information classified under the authority of Executive Order 12958 as amended or any predecessor Order is protected from unauthorized disclosure, and that the granting of access to classified information or assignment to other sensitive duties is clearly consistent with the interests of national security.

1001. Objectives. The MCAS Yuma IPSP is designed to accomplish the following:

1. Prevent unauthorized persons from gaining access to classified information.
2. Provide security for classified information consistent with those requirements established by higher authority and sound management principles.
3. Develop information and personnel security awareness and practices through education and training.

1002. Responsibility for Compliance

1. Commanding Officers and Department Heads are responsible for compliance and implementation of the MCAS Yuma IPSP within their respective organizations.
2. Each individual, military or civilian, in the Navy or Marine Corps, is responsible for complying with all aspects of this program, and is charged with the responsibility of reporting all violations or suspected violations of this Order directly to the Command Security Manager or Assistant Security Manager.

1003. Policy Guidance. Requests for guidance/interpretation concerning the contents of this Order should be directed to the Mission Assurance Department (MAD).

CHAPTER 2

COMMAND SECURITY MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
Command Security Responsibility and Implementation	2000	2-2
Command Security Manager	2001	2-3
Assistant Security Manager	2002	2-3
Duties of the Security Manager/ Assistant Security Manager	2003	2-3
Secondary Control Point (SCP) Custodian	2004	2-5
Other Security Appointments	2005	2-6
All Hands	2006	2-7
Security Reviews and Inspections	2007	2-7
Planning for Emergencies	2008	2-7
Internal Security Procedures	2009	2-8

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. Command Security Responsibility and Implementation

1. The Commanding Officer is ultimately responsible for the implementation and effective management of the IPSP aboard MCAS Yuma. The Commanding Officer will appoint, in writing, a Security Manager and Assistant Security Manager to carry out the requirements and procedures for the IPSP.

2. Command Security Management responsibilities include:

a. Issue written command security procedures.

b. Issue an emergency plan for the protection of classified information in emergency situations.

c. Ensure that command security inspections, program reviews, and assist visits to Secondary Control Points (SCPs) are conducted at least annually.

d. Apply risk management, as appropriate, for the safeguarding of classified information, and monitor its effectiveness in the command.

e. Establish an industrial security program to provide security oversight over classified work carried out by cleared DoD contractors operating aboard MCAS Yuma.

f. Ensure that the Security Manager and other command security professionals receive training as required, that all personnel receive required security education, and that the command has a robust security awareness program.

g. Ensure that the performance rating systems of all military and civilian personnel who have access to classified information includes a comment from the Reporting Senior/Rating Official about the individual's suitability for continued access to classified information.

h. Ensure command personnel are aware that they are expected and encouraged to challenge the classification of information that they believe to be improperly classified, and that procedures for challenging and appealing such status are

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

understood.

3. This directive establishes a network of security professionals throughout the command to ensure effective security management (see paragraphs 2001 through 2007).

2001. Command Security Manager

1. The Director, Mission Assurance Department will be designated in writing as the Command Security Manager (see figure 2-1). The Security Manager is the principal advisor on information and personnel security in the command and is responsible to the Commanding Officer for the proper management of the program.

2. The Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the previous 5 years.

3. The Security Manager must complete the Naval Security Manager Course offered by the Naval Criminal Investigative Service Security, Training, Assistance, and Assessment Team as soon as practicable after designation.

2002. Assistant Security Manager

1. The Assistant Security Manager will be designated in writing and be assigned to the Mission Assurance Department (see figure 2-1). The Assistant Security Manager carries out the day to day provisions of the Information and Personnel Security Program at MCAS Yuma, and is responsible to the Command Security Manager for ensuring the program is inclusive of all requirements. Additionally, the Assistant Security Manager will act in place of the Security Manager during his/her absence.

2. The Assistant Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI completed within the previous 5 years.

2003. Duties of the Security Manager/Assistant Security Manager

1. The Command Security Manager and Assistant Security Manager are responsible for implementing the IPSP at MCAS Yuma, and will be identified to all members of the command on organization charts, telephone listings, rosters, etc.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

2. The duties and responsibilities of the Command Security Manager/Assistant Security Manager, as outlined in the references, include:

a. Serve as the principal advisor and representative to the Commanding Officer in matters pertaining to the security of classified information held at the command.

b. Serve as the principal advisor and representative to the Commanding Officer in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

c. Develop written command information and personnel security procedures, including an emergency plan for the protection of classified material during emergency situations. Guidance for developing an emergency plan is contained in Exhibit 2B of reference (b).

d. Ensure that personnel in the command who perform security duties are kept abreast of changes in policies and procedures, and provide assistance in problem solving.

e. Formulate, coordinate, and conduct the command's security awareness and education program as outlined in Chapter 4 of this Order.

f. Ensure that threats to security, and other security violations are reported, recorded, and, when necessary, investigated. Ensure that all incidents involving loss, compromise, or possible compromise of classified information are immediately referred to the nearest Naval Criminal Investigative Service (NCIS) office, and a Preliminary Inquiry (PI) is conducted.

g. Maintain liaison with the command Public Affairs Officer (PAO) to ensure that proposed press releases and information intended for public release are subjected to a security review (see Chapter 8 of reference (b)).

h. Coordinate with other command officials regarding security measures for the classification, safeguarding, transmission, and destruction of classified information.

i. Ensure security control of visits to and from the command when the visitor requires, and is authorized, access to classified information. The Joint Personnel Adjudication System

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

(JPAS) will be the primary vehicle for this action.

j. Implement and interpret, as needed, regulations governing the disclosure of classified information to foreign governments.

k. Ensure compliance with all regulatory requirements when access to classified information is provided to industry in connection with a classified contract.

l. Coordinate with the Command Information Assurance Manager on matters of common concern.

m. Ensure that access to classified information is limited to appropriately cleared personnel with a "need-to-know".

n. Ensure that requests for personnel security investigations are properly prepared, submitted, and monitored.

o. Ensure that personnel security investigations, clearances and accesses are properly recorded.

p. Ensure that all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information.

q. Ensure that all personnel who have had access to classified information who are separating or retiring have completed a Security Termination Statement (OPNAV 5511/14). See paragraph 4005.

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

2004. Secondary Control Point (SCP) Custodian

1. Each staff section that has been authorized to receipt for and store classified material is classified as a SCP. The department head will designate, in writing, a SCP Custodian and an alternate (see figure 2-3). This appointment will be a commissioned or warrant officer, enlisted E-5 or above, or GS-05 or above. A copy of the appointment letter will be forwarded to the MAD.

2. Personnel appointed as SCP Custodian or alternate custodian will certify that they have completed a sight inventory of all

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

classified material maintained in the SCP.

3. The SCP Custodian, or in their absence, the alternate custodian, is the department/section representative responsible for implementing and maintaining required controls of all classified information held by or routed to the division or section. This includes:

- a. Receipt.
- b. Routing.
- c. Maintenance of up-to-date records of materials held.
- d. Destruction.
- e. Reproduction.
- f. Ensuring that only authorized persons have access to classified material.
- g. Promulgation and periodic review of policy and procedures for the control of classified material within the SCP.

2005. Other Security Appointments

1. Electronic Key Management System (EKMS) Custodian. See reference (d).
2. Information Assurance Manager (IAM). See reference (e). The IAM is an Automated Information System (AIS) I Sensitive Position (see Chapter 5) and requires a favorably adjudicated SSBI completed within the previous 5 years.
3. Physical Security Officer. See reference (f).
4. Contracting Officer's Representative (COR). A COR will be designated for each classified contract per reference (b). The COR is responsible to the Security Manager for coordinating with program managers and procurement officials. The COR will ensure that the industrial security functions specified in reference (b) and Chapter 17 of this Order are accomplished when classified information is provided to industry for performance on a classified contract.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

2006. All Hands. Security is the responsibility of all personnel. Each individual who handles classified material is responsible for ensuring that the material is properly safeguarded, properly stored, and that access is given only to authorized personnel. Personnel who do not handle classified material must be alert to and immediately report any instances of unauthorized access.

2007. Security Reviews and Inspections

1. The Security Manager/Assistant Security Manager will conduct an internal security review annually of the Station Information and Personnel Security Program using the self-inspection guides found in Appendix D of reference (a) and Exhibit 2C of reference (b) as well as the current Marine Corps Automated Inspection Reporting System Checklist.

2. SCP Custodians will conduct annual security reviews to evaluate the overall security posture of their respective areas, using Figure 2-4 as a guide. As a minimum, security reviews will include an inventory of all classified holdings, clearance verification, and handling/storage requirements of classified information.

3. The MAD will inspect SCPs on an annual basis to assess compliance with the requirements for handling classified material per reference (b) and this order.

4. Copies of the completed SCP inspection checklist will be provided to the appropriate SCP Custodian. Inspection reports will be kept on file by the SCP custodian for two years.

5. If discrepancies are noted, the SCP will be reinspected in 30 days to ensure appropriate corrective action has been completed. If upon reinspection it is determined that corrective action has not been taken, a Preliminary Inquiry may be ordered which may result in punitive action as appropriate.

2008. Planning for Emergencies

1. Per references (a) and (c), each command is required to establish a plan for the protection and removal of classified National Security Information (NSI) under its control during emergencies. The MAD will develop and maintain the emergency action plan (EAP) for MCAS Yuma. The EAP will be maintained within the Mission Assurance Department.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

2. In addition, each SCP will develop an EAP for the protection and removal of classified NSI maintained in the SCP in case of natural disaster, civil disturbance, or enemy action. These plans will detail specific procedures and responsibilities for each SCP. These plans will be maintained within the MAD and the respective SCP.

2009. Internal Security Procedures

1. Each department which handles and stores classified information will prepare and keep current written security procedures specifying how the requirements of this order will be accomplished within their department. The MAD is available to assist in the drafting of these documents.

2. Internal security procedures should include, but are not limited to: accounting and control of classified information, physical security measures, control of reproduction, destruction, screening of incoming material until a security determination has been made, requesting and recording security clearances, security education, inspections, 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 Station Order P5510.3" are not considered adequate for internal security procedures.

4. A copy of the internal security procedures will be forwarded to the MAD.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

COMMAND LETTERHEAD

5510
MAD
(Date)

From: Commanding Officer
To: Grade Name, SSN (last 4 only)/MOS, USMC
Subj: DESIGNATION AS STATION SECURITY MANAGER/ASSISTANT
SECURITY MANAGER
Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.18
(d) StaO P5510.30

1. In accordance with the references, you are hereby designated as the Station Security Manager/Assistant Security Manager for Marine Corps Air Station Yuma. You will be governed in your duties by the reference and other applicable directives. You are directed to thoroughly familiarize yourself with them.
2. By endorsement of this letter you will certify that you are familiar with your responsibilities as the Station Security Manager.
3. This designation supersedes all previous appointments.

SIGNATURE

(Date)

FIRST ENDORSEMENT

From: Grade, Name, SSN (last 4 only)/MOS, USMC
To: Commanding Officer

1. I have read and understand the provisions of the references and assume the duties as the Security Manager/Assistant Security Manager for Marine Corps Air Station Yuma.

SIGNATURE

Copy to:
MCAS Yuma MAD

Figure 2-1. Sample Security Manager/Assistant Security
Manager Appointment Letter

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

COMMAND LETTERHEAD

5510
Dept Code
(Date)

From: Commanding Officer
To: Grade Name, SSN (last 4 only)/MOS, USMC
Subj: APPOINTMENT AS PERSONNEL SECURITY COORDINATOR
Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.18
(d) StaO P5510.30

1. In accordance with reference (a), you are appointed as the Personnel Security Coordinator for (Department). You will familiarize yourself with the requirements of the Information and Personnel Security Programs set forth in the references. Further, you are directed to contact the Mission Assurance Department (MAD) for guidance on your duties.
2. You will coordinate program requirements with the MAD and will provide (Department) personnel assistance as required.
3. You will indicate by endorsement below that you are ready to assume the duties as the (Department) Personnel Security Coordinator.

SIGNATURE

(Date)

FIRST ENDORSEMENT

From: Grade, Name, SSN (last 4 only)/MOS, USMC
To: . Department Head

1. I am familiar with the requirements of the Information and Personnel Security Programs set forth in the references, and have assumed my duties as the (Department) Personnel Security Coordinator.

SIGNATURE

Copy to:
MAD

Figure 2-2. Sample Personnel Security Coordinator
Appointment Letter

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

COMMAND LETTERHEAD

5510
Dept Code
(Date)

From: Department Head
To: Grade, Name, SSN (last 4 only)/MOS, USMC
Subj: APPOINTMENT AS SECONDARY CONTROL POINT CUSTODIAN/ALTERNATE
CUSTODIAN

Ref: (a) StaO P5510.30
(b) SECNAV M-5510.30
(c) SECNAV M-5510.36
(d) MCO P5510.18

1. In accordance with reference (a), you are appointed as the Secondary Control Point (SCP) Custodian/Alternate Custodian for the (Department/Section) per reference (a). You will familiarize yourself with all pertinent publications and instructions concerning classified material, including the references.

2. You will conduct a sight inventory of all classified material maintained at this SCP and report the results by endorsement to this letter. After all classified material has been inventoried and accounted for, you will assume the duties as the (Department/Section) Secondary Control Point Custodian/Alternate Custodian.

SIGNATURE

(Date)

FIRST ENDORSEMENT

From: Grade, Name, SSN (last 4 only)/MOS, USMC
To: Department Head

1. I have read and understand the provisions of the references. All classified material maintained by this SCP has been inventoried and accounted for. I have assumed my duties as the (Department/Section) Secondary Control Point (SCP) Custodian/Alternate Custodian.

SIGNATURE

Copy to:
MAD

Figure 2-3. Sample Secondary Control Point Custodian/Alternate Custodian Appointment Letter

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

SCP SECURITY REVIEW CHECKLIST

1. Is there an authorization letter signed by the Command Security Manager on file establishing the Secondary Control Point (SCP)?
2. Is there a current appointment letter on file for the SCP Custodian and Alternate Custodian?
3. Is there a current security clearance access listing on file?
4. Are only personnel who have been granted access to classified areas in writing authorized access to those areas?
5. Do all personnel know who the Security Manager and Assistant Security Manager are?
6. Are all personnel aware of their requirement to report all derogatory information known about anyone within their work section directly to the Command Security Manager or Assistant Security Manager?
7. Have safe combinations been changed as required by SECNAV M-5510.36?
8. Is there a current SF 700 envelope on file in the MAD that reflects the latest combination changes?
9. Is the Activity Security Checklist, SF 701, and Security Container Check Sheet, SF 702, being properly used?
10. Does the SCP have a copy of the current SECNAV M-5510.36, SECNAV M-5510.30, and Station Order P5510.3?
11. Are personnel familiar with the safeguarding requirements for classified information and what to do in the event of loss, compromise, or possible compromise of classified information?
12. Have there been any security violations since the last security review?
13. Have all personnel attended all required security training (i.e., annual refresher briefings, counter-intelligence briefings, anti-terrorism training)?
14. Is on-the-job training being provided as required?

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	3000	3-2
Activities to be Reported	3001	3-2

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

3000. Basic Policy

1. All station personnel, military and civilian, whether they have access to classified information or not, will report to appropriate personnel any activities affecting national security involving themselves, their families, co-workers, or others.

2. Appropriate personnel include the Command Security Manager, Assistant Security Manager, the appropriate Department Head, the Department Personnel Security Coordinator, the individual's supervisor, any other person in the individual's chain of command, and the nearest command if away from MCAS Yuma. If the information is reported to an individual other than the Command Security Manager, that individual is responsible for notifying the Command Security Manager of all available information as soon as possible.

3. The Command Security Manager and Assistant Security Manager are the command representatives for notifying the NCIS Resident Agency (NCISRA), MCAS Yuma so appropriate counterintelligence action can be taken. If personnel desire, they may notify NCIS directly at (928) 269-2305, or the Espionage Hotline at 1-800-543-NAVY (6289).

3001. Activities to be Reported. The following is a listing of the activities that must be reported to NCIS. These activities are described in further detail in Chapter 3 of reference (a).

1. Sabotage, Espionage, Terrorism or Deliberate Compromise. Command personnel becoming aware of possible acts of sabotage, malicious damage, espionage, terrorism, deliberate compromise, or other subversive activities will report all available information immediately to appropriate personnel.

2. Contact Reporting. Command personnel who possess a security clearance will report to appropriate personnel contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

3. Suicide or Attempted Suicide. Command personnel who become aware of a suicide or attempted suicide by a member of the command who has had access to classified information will report all available information immediately to appropriate personnel. Additionally, the department head of the individual involved will forward a written report to the Security Manager of the extent and nature of classified information to which the individual had access.

4. Unauthorized Absentees. Command personnel who become aware of an unauthorized absence by a member of the command who has had access to classified information will report all available information immediately to appropriate personnel. Additionally, the department head of the individual involved will conduct an inquiry to determine if there are any indications from the absent individual's activities, behavior, or associations that the absence may be contrary to the interests of national security. If there are such indications, a report will be forwarded immediately to the Command Security Manager.

5. Death or Desertion. When a member of the command who has had access to classified information dies or deserts, the department head of the individual involved will determine if there are any unusual indicators or circumstances that may be contrary to the interests of national security. If such conditions exist, a report will be forwarded immediately to the Command Security Manager.

6. Foreign Connections. All personnel with established security clearance eligibility are required to report foreign connections to the MAD.

CHAPTER 4
SECURITY EDUCATION PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	4000	4-2
Responsibilities	4001	4-2
Security Briefings	4002	4-2
Additional Specialized Training	4003	4-4
Command Debriefing	4004	4-4
Security Termination Statement	4005	4-5
Continuing Security Awareness	4006	4-6
Records	4007	4-6

CHAPTER 4

SECURITY EDUCATION PROGRAM

4000. Basic Policy. The purpose of security education is to ensure that all personnel, regardless of position, rank, or grade, understand the need and procedures for protecting classified and sensitive unclassified information. The goal is to develop fundamental security habits as a natural element of each task. Detailed procedures on establishing a command security education program are set forth in Chapter 4 of reference (a).

4001. Responsibilities

1. The Command Security Manager is responsible for the overall security education program in the command and for ensuring sufficient time is dedicated for training and awareness.
2. The Assistant Security Manager is responsible for ensuring the security education program provides for the minimum briefing requirements listed below, and for developing and coordinating command indoctrination, orientation, and refresher briefings.
3. Departments are responsible for coordinating all security related training with the MAD. The MAD will maintain accurate files of completed training.
4. Department heads are responsible for identifying the security requirements within their area of responsibility and for ensuring personnel under their supervision understand the security requirements for their particular assignment. On-the-job training is an essential part of the security education program, and supervisors must ensure that such training is provided.

4002. Security Briefings

1. Indoctrination. Military personnel entering the Marine Corps receive a basic indoctrination during accession training in the basic principles of security. The MAD will conduct security indoctrination training for new civilian employees being employed by the Department of the Navy for the first time.
2. Orientation. An orientation briefing will be given to all personnel who will have access to classified information as soon as possible after reporting aboard or being assigned to duties

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

involving access to classified information. The briefing will include the command security structure (i.e., who the security manager is, etc.); any special security precautions within the command (e.g., restrictions on access); and their general security responsibilities. The MAD is responsible for this briefing.

3. On-the-Job Training. Supervisors must ensure subordinates know the security requirements impacting on the performance of their duties. This training may consist of oral reminders, meetings, or written instructions. Supervision of the on-the-job training process is critical. Supervisors are ultimately responsible for procedural violations or for compromises that result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable.

4. Annual Refresher Briefing. A security refresher briefing will be given annually to all command military and civilian personnel who have access to classified information. The briefing will cover new security policies and practices, counterintelligence reminders, continuous evaluation, security concerns or problem areas, and security safeguards and measures to protect classified and sensitive unclassified information. Other security-related topics may be included as necessary. The MAD is responsible for this briefing.

5. Counterintelligence Briefings. All personnel who have access to material classified Secret or above must be given a counterintelligence briefing by a Naval Criminal Investigative Service (NCIS) agent once every two years. NCIS will normally provide this brief on a quarterly basis. The MAD will coordinate with NCIS and departments for scheduling these briefings.

6. Special Briefings. The MAD will arrange for any special briefings personnel require as circumstances dictate, including:

a. Foreign Travel Briefing. This briefing will normally be given as part of the annual refresher brief. A classified version may also be given on an individual basis upon request to those individuals with access to classified information who are traveling to a foreign destination.

b. New Requirements Briefing. Personnel whose duties would be impacted by changes in security policies or procedures will

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

be briefed as soon as possible.

c. Program Briefings. Personnel who require access to a unique program (i.e., NATO, CNWDI, or SCI) will be briefed on the program's requirements as the need arises.

d. Training for Derivative Classifiers. The MAD will train derivative classifiers on an as required basis.

e. Training for Classified Couriers. The MAD will train classified couriers per reference (b), on an as required basis.

4003. Additional Specialized Training. In addition to the requirements listed above, specialized training is required for the following:

1. Security Manager and Assistant Security Manager. These individuals will complete the Naval Security Manager Course offered by the Naval Criminal Investigative Service Security, Training, Assistance, and Assessment Team as soon as practicable after designation.

2. SCP Custodians and Alternate Custodians. Indoctrination training in accountability and safekeeping requirements for classified information is mandatory for all newly appointed SCP Custodians and alternate custodians. It must be completed within three months following their appointment. Personnel will coordinate with the MAD for scheduling of this training.

4004. Command Debriefing

1. All personnel checking out of the command, including those transferring to another command, terminating active military service or DoD civilian employment, going on terminal leave, or temporarily separating for a period of 60 days or more, will check out with the MAD.

2. The MAD will debrief departing personnel on any check-out procedures pertaining to the individual's duties. In addition, the individual will be instructed that all classified information personally compiled, such as notes and notebooks, for which a legitimate need can be determined at the gaining command, must be forwarded through official command channels by the MAD.

3. The Command Assistant Security Manager, or designated representative, will debrief personnel who no longer require

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

access to classified information when any of the following occur:

- a. Transfers from one command to another (unless it is known that the individual will require access to classified material by the gaining command);
- b. Terminating active military service or civilian employment;
- c. Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or transfer to the Inactive Ready Reserves (IRR);
- d. Expiration of a Limited Access Authorization (LAA);
- e. Inadvertent substantive access to information that the individual is not eligible to receive;
- f. Security clearance eligibility revocation;
- g. Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause.
- h. DoD civilian employees temporarily separating for a period of 60 days or more, including sabbaticals and leave without pay status.
- i. Inadvertent substantive access to classified information that the individual was not eligible to receive.
- j. Administrative withdrawal or suspension of security clearance.

4005. Security Termination Statements

1. Personnel who no longer require access to classified information as a result of any of the activities listed in paragraph 4004 herein, must read and execute a Security Termination Statement (OPNAV 5511/14) at the time of debriefing by the MAD.
2. The original signed and witnessed Security Termination Statement will be placed in the individual's official service record or official personnel folder for permanent retention and copy retained by MAD, except in certain situations described in reference (a). However, for uniformed Marine personnel

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

separating or retiring, MAD will mail the ORIGINAL to the Commandant of the Marine Corps (MMSB-20), 2008 Elliot Road, Quantico VA 22134-5030.

3. If an individual refuses to sign the Security Termination Statement, the MAD or designated representative will still debrief the individual and will inform the individual that refusal to sign does not negate the obligation never to divulge classified information to an unauthorized person. The MAD or designated representative will annotate on the Security Termination Statement that the individual was debriefed, but refused to sign, and send a copy to CMC (MMSB).

4006. Continuing Security Awareness. The previous paragraphs describe the minimum briefing requirements for the command's security education program. To enhance security in a continuing and evolving program, personnel should be frequently exposed to current information. Signs, posters and bulletin board notices are some of the media that should be used to boost security awareness. These materials are available from the MAD. Security Manager notes sent via e-mail also help to reinforce the security education program.

4007. Records. The Assistant Security Manager will maintain appropriate records of the type of security education conducted within the command, with attendance dates and rosters. These records will be maintained for two years.

CHAPTER 5
NATIONAL SECURITY POSITIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	5000	5-2
Designation of Sensitive Positions	5001	5-2
Criteria for Designating Sensitive Positions	5002	5-3
Suitability and Security Determinations	5003	5-6

CHAPTER 5

NATIONAL SECURITY POSITIONS

5000. Basic Policy

1. National Security Positions are those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage and positions that require regular use of, or access to, classified information.

2. Title 5 Code of Federal Regulations (CFR) 732.201 requires that positions identified as National Security Positions be assigned a position sensitivity level.

5001. Designation of Sensitive Positions

1. A sensitive national security position is any position whose occupant could bring about, by virtue of the nature of the position, an adverse effect on the national security. There are three sensitivity levels (and one non-sensitive level) that apply to national security positions:

- a. Special-Sensitive (SS).
- b. Critical-Sensitive (CS).
- c. Noncritical-Sensitive (NCS).
- d. Non-Sensitive (NS).

2. Each National Security Position (DoD civilian position) in the command will be designated as special-sensitive, critical-sensitive, or noncritical-sensitive. Any civilian position not designated as a sensitive national security position will be by default a non-sensitive position.

3. Department Heads, in coordination with the Security Manager/Assistant Security Manager and the Human Resources Office, will designate a position sensitivity level for each national security position (henceforth referred to as "sensitive" positions) under their control. The Director, Communications Data Electronics Department, is responsible for designating positions according to their Information Technology

risk level.

5002. Criteria for Designating Sensitive Positions

1. It is vital that great care be taken when selecting individuals to fill sensitive positions. Each Position Description (PD) and Job Announcement for sensitive positions will include the position sensitivity and security clearance requirement. Failure to attain and maintain the security clearance requirement for the position will result in the individual being removed from the position.

2. Positions that meet one or more of the following criteria will be designated as sensitive:

a. Special-Sensitive (SS): Any position which the head of an agency determines to be at a level higher than Critical Sensitive:

(1) Due to the greater degree of damage to the national security that an individual could effect by virtue of his/her position, or

(2) Special requirements concerning the position under authority other than E.O. 10450, such as designations applied under SSO cognizance pertaining to DCID 6/4.

(3) No positions at MCAS Yuma are currently designated as Special Sensitive.

b. Critical-Sensitive (CS): Any position that includes:

(1) Access to Top Secret national security information.

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

(3) Fiduciary, public contact, or other duties demanding the highest degree of public trust. (Fiduciary duties involving IT systems are also designated as IT positions as described below.)

(4) Certain IT positions will be designated as CS, and IT-I, due to the potential for grave damage to the national security. CS IT-I positions include those in which the incumbent

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

has:

(a) Responsibility for development and administration of computer security programs, and also including direction and control of risk analysis and/or threat assessment.

(b) Been designated as IAM or IAO.

(c) Significant involvement in life-critical or mission-critical systems.

(d) Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(e) Relatively high risk assignments associated with or directly involving the accounting, disbursement or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by a higher authority in the IT-I category to insure the integrity of the system.

(f) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and/or management of systems hardware and software.

(g) Other IT positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

c. Noncritical-Sensitive (NCS): Any position that involves:

(1) Access to Secret or Confidential national security information.

(2) Assignment to duties involving the protection and safeguarding of DON personnel and property (e.g., security police, provost marshal, duties associated with ammunitions and arms).

(3) Duties involving the education and orientation of DoD personnel. (Applicable only to personnel who prepare formal instructional material or present formal courses of

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

instruction.)

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

(5) Responsibility for financial operations subject to routine supervision or approval, but with no funds disbursement or transfer capabilities. (Fiduciary duties involving IT systems are also designated as IT positions as described below.)

(6) Non-management DON mission support positions with authority for independent or semi-independent action.

(7) Duties involving delivery of service to support the DON mission requiring confidence or trust.

(8) Certain IT positions will be designated as NCS, and IT-II, due to the potential for serious damage to the national security. NCS IT-II positions include those in which the incumbent has:

(a) Responsibility for systems design, operations, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the CS IT-I category.

(b) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems, system security and network defense systems, or to system resources providing visual access and/or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny sensitive information.

(c) Duties associated with or directly involving the accounting, disbursement or authorization for disbursement of funds in dollar amounts of less than \$10 million per year; and/or duties that involve the development, writing and administration of, and/or awarding, approving or modifying of contracts which total dollar amounts less than \$10 million per year; or as deemed appropriate by the agency head those commensurate fiscal duties with potential for damage or personal gain.

(d) Other positions as designated by the agency head that involve a degree of access to a system that creates a

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

potential for serious damage or personal gain less than that in CS IT-I positions.

d. All other civilian positions in the DON are designated as non-sensitive, including category III AIS positions. A security clearance will not be granted to an individual in a non-sensitive civilian position.

3. The position sensitivity will be determined for every DOD civilian position in the command and recorded in the Defense Civilian Personnel Data System (DCPDS). DCPDS will serve as the command's source document for identifying position sensitivities. The MAD will only submit civilian personnel for security investigations commensurate with the position sensitivity recorded in DCPDS.

5003. Suitability and Security Determinations

1. Non-Sensitive Positions. Investigations for non-sensitive positions require only an employment suitability determination. Command responsibility for employment suitability adjudication for DOD civilians in non-sensitive positions is delegated to the HRO, per the standards and criteria established by the Office of Personnel Management (OPM) and contained in Title 5 CFR 731.

2. Sensitive Positions. Investigations for sensitive positions require both an employment suitability determination and a security determination.

a. Security determinations for DOD civilians in sensitive positions are usually made by the Department of the Navy Central Adjudication Facility (DON CAF) based on criteria found in reference (a).

b. The DON CAF has been delegated the authority to make de facto suitability determinations only on investigations closed without actionable issues. In cases without issue, a favorable security determination equates to a favorable suitability determination.

c. If the DON CAF determines there are suitability issues associated with an investigation submitted for a sensitive position, the DON CAF will forward it to the command for suitability adjudication. If the command makes a favorable suitability determination, the investigation will be returned to DON CAF to make a security clearance eligibility determination. If the suitability determination made by the command is

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

unfavorable, it remains a personnel action and no DON CAF action is required. See reference (a) for further guidance.

CHAPTER 6

PERSONNEL SECURITY INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	6000	6-2
Types of Personnel Security Investigations	6001	6-2
Investigative Requirements	6002	6-2
Submission Requirements	6003	6-4
Preparation and Submission of Investigative Requests	6004	6-5
Follow-up Actions on Investigative Requests	6005	6-5

CHAPTER 6

PERSONNEL SECURITY INVESTIGATIONS

6000. Basic Policy

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability, and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations.

2. Only the minimum investigation necessary to satisfy the requirements for the level of access required or sensitivity of position occupied will be requested.

3. PSIs will not normally be requested for any civilian or military personnel who will be retired, resigned, or separated with less than one year service remaining.

4. DON CAF assigns clearance eligibility at the highest level supportable by the investigation completed. The access granted is a local command responsibility, and is based on need-to-know established by the CO, not the individual requesting access. Access will not be granted automatically and does not have to be granted at the level of eligibility.

6001. Types of Personnel Security Investigations. The types of personnel security investigations conducted by the Office of Personnel Management (OPM) for the DON are described in reference (a).

6002. Investigative Requirements

1. Personnel Security Clearances

a. Only U.S. citizens are eligible for security clearances. Thus, investigation requests will only be submitted on individuals verified to be a U.S. citizen.

b. Security clearance eligibility will be based on a PSI prescribed for the level of classification.

(1) Top Secret. The investigative basis for Top Secret clearance eligibility is a favorably completed Single Scope Background Investigation (SSBI) or Periodic Reinvestigation

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

(PR). For those who have continuous assignment or access to Top Secret, critical sensitive positions, SCI, or Presidential Support Activities, the SSBI must be updated every five years by a PR.

(2) Secret/Confidential. The investigative basis for Secret or Confidential clearance eligibility is a favorably completed National Agency Check with Local Agency and Credit Checks (NACLCC) for military personnel or Access National Agency Check with Written Inquiries (ANACI) for DOD civilian personnel.

(a) For Secret clearances, the investigation must be updated every ten years by a NACLCC. As an exception, NACLCCs are required every five years for personnel in Special Access Programs (SAPs) with access to Secret classified military information (CMI), and those performing Explosive Ordnance Disposal (EOD) or Personnel Reliability Program (PRP) duties.

(b) For Confidential clearances, the investigation must be updated every 15 years by a NACLCC.

c. All military and civilian investigation requests, except as noted in paragraph 2 below, will be completed via the electronic Questionnaires for Investigations Processing (e-QIP). Accurate and timely completion of a request is the individual's responsibility. MAD is available for assistance.

2. Civilian Employment in Sensitive Positions

a. The type of investigation required for civilian employees of the DON depends on the sensitivity level of the position the employee is appointed to, as follows:

- (1) Nonsensitive position - NACI
- (2) Noncritical-Sensitive position - ANACI
- (3) Critical-Sensitive position - SSBI
- (4) Special-Sensitive position - SSBI

b. The Human Resources Office is responsible for submitting investigation requests to determine suitability for federal employment of civil service employees appointed to non-sensitive positions. They will submit the appropriate investigation request on employees new to federal employment or who have had more than a 24-month break in employment, per the requirements

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

specified in reference (a). The HRO will coordinate requirements for security clearances with MAD as required.

3. Specific Performance of Duty and Special Programs. The investigative requirements for personnel performing specific duties (e.g., Security Manager, cryptographic duties, and IT duties) and those mandated for certain programs (e.g., SCI, NATO) are described in reference (a). These requirements will be coordinated with the MAD as necessary.

6003. Submission Requirements. Before submitting a PSI request to OPM, the MAD will ensure completion of the following procedures:

1. Verification of Prior Investigation

a. Determine if the required investigation already exists. This is accomplished by checking the Joint Personnel Adjudication System (JPAS). (Note: Per MARADMIN 106/00, the Marine Corps Total Force System (MCTFS) will not be used for verification of security clearances or access eligibility).

b. A PSI request must be submitted if:

(1) There is no investigative basis present;

(2) There has been a break in service greater than 24 months since the date of the individual's last investigation; or

(3) The individual is due for a reinvestigation per paragraph 6002 herein.

2. Local Records Check (LRC). An LRC consists of a review of available personnel, medical, legal, security, base/military police, and other command records to determine if locally available disqualifying information exists.

3. Validate Citizenship. The MAD will verify that the individual is a United States citizen, using the guidelines contained in reference (a).

4. Verify Date and Place of Birth and Education. When requesting an SSBI, the MAD will verify, if possible, the individual's date and place of birth and most recent or most significant claimed education. A birth certificate or available personnel records may be used to verify the date and place of

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

birth. A diploma or transcript may be used to verify education.

6004. Preparation and Submission of Investigative Requests

1. Personnel will complete a PSI request using the Electronic Questionnaire for Investigations Processing (e-QIP) software.
2. Investigative requests will be completed per guidance provided by the MAD.
3. The MAD will review and validate the investigation request forms for completeness and accuracy, and will transmit the completed, validated, and signed PSI request to the appropriate investigative agency (OPM).
4. MAD will maintain a pdf copy of the PSI request for future tracer actions until DON CAF adjudication is complete.
5. If an individual refuses to provide or permit access to relevant information for investigative purposes, the Command Security Manager/Assistant Security Manager will advise the individual of the effects of refusal. If the individual still refuses, the PSI request process will be terminated. The individual will not be eligible for access to classified information or assignment to sensitive duties unless the information is made available. If the individual is currently cleared for access to classified information and/or is performing sensitive duties, the Security Manager/Assistant Security Manager will refer the matter to the DON CAF for action.

6005. Follow-up Actions on Investigative Requests. MAD will conduct follow-up actions with OPM as needed until the investigation is complete and DON CAF makes the clearance determination, per reference (a).

1. If an investigation is in a pending status and the individual is released from active duty, discharged, resigns, or when circumstances change that negate the need for the investigation, the investigation is to be promptly cancelled. The MAD will notify DON CAF accordingly.
2. Tracer actions for Marines must be submitted to the DON CAF.

CHAPTER 7

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	7000	7-2
Personnel Security Program Responsibilities	7001	7-2
Personnel Security Determinations	7002	7-3
Unfavorable Determination Process	7003	7-4
Appealing Unfavorable Determinations	7004	7-4

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CHAPTER 7

PERSONNEL SECURITY DETERMINATIONS

7000. Basic Policy

1. No person will be entrusted with classified information or assigned to sensitive duties unless it is clearly consistent with the interests of national security.
2. Security clearance eligibility or assignment to sensitive duties will be based on a determination of the individual's loyalty, reliability, and trustworthiness, and will be governed by the provisions of this order and reference (a).
3. A determination to grant security clearance eligibility, authorize access to classified information, or assign an individual to sensitive duties will be based on a common sense evaluation of all available information, favorable and unfavorable, assessed for accuracy, completeness, relevance, importance and overall significance.
4. Personnel security policies and procedures apply primarily to eligibility for access to classified information or assignment to sensitive duties. Unless there is a reasonable basis for doubting a person's loyalty to the Government of the United States, decisions regarding appointment or retention in civilian employment or acceptance or retention in the Navy and Marine Corps are governed by personnel policies not under the purview of the IPSP.

7001. Personnel Security Program Responsibilities

1. Central Adjudication. The Department of the Navy Central Adjudication Facility (DON CAF) adjudicates information from personnel security investigations and other relevant information, and determines eligibility for security clearances and SCI access, and/or assignment to sensitive duties for all DON personnel, civilian and military.
2. Command Responsibilities. The Command Security Manager and Assistant Security Manager have personnel security jurisdiction over all departments and staff sections. They are responsible for reviewing locally available information pertinent to personnel security determinations; keeping DON CAF informed of all matters impacting on an individual's eligibility for a clearance and/or assignment to a sensitive position; and will

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

ensure the command responsibilities listed in reference (a) are carried out.

7002. Personnel Security Determinations

1. A personnel security determination is required when:

a. A personnel security investigation on a nominee for a security clearance or assignment to sensitive civilian duties has been completed.

b. Access to classified information or assignment to sensitive duties is necessary under interim conditions.

c. Questionable or unfavorable information becomes available about an individual in a sensitive position or a position requiring access to classified information.

d. The issues that prompted a previous unfavorable personnel security determination no longer exist and the individual is again being considered for clearance or assignment to sensitive duties.

2. When determining eligibility for access to classified information or assignment to sensitive duties, the DON CAF uses the adjudication criteria contained in reference (a) to evaluate information in available personnel security investigative files and from other sources, including personnel, medical, legal, law enforcement, and security records.

3. Derogatory information about an individual assigned to or employed by this command may be received under the Continuous Evaluation Program (see reference (a) and Chapter 10 of this Order); discovered during a LRC; or included on a PSI request.

a. Upon receipt of such information, the Command Security Manager/Assistant Security Manager will determine if the information is of such magnitude that it may adversely affect the individual's ability to properly safeguard classified information or perform sensitive duties.

b. If this is the case, the Commanding Officer, on the recommendation of the Command Security Manager/Assistant Security Manager, will determine whether, on the basis of all the facts, to suspend or limit an individual's access to classified information, or reassign the individual to non-

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

sensitive duties pending a final determination by the DON CAF.

c. The Command Security Manager/Assistant Security Manager will provide the rationale for their recommendation in writing; and will coordinate their recommendation with other appropriate personnel (e.g., the individual's department head), HRO personnel (if a civilian employee is involved), who will consider and evaluate the information. It is essential that all those directly involved in this evaluation process take an objective approach to ensure consideration of individual and the protection of national security.

7003. Unfavorable Determination Process. When DON CAF is contemplating an unfavorable personnel security determination, the DON CAF issues to the individual concerned, via the individual's command, a Letter of Intent (LOI) to revoke or deny security clearance eligibility, SCI access or sensitive position eligibility. The Command Security Manager or Assistant Security Manager will coordinate and adhere to the procedures delineated in reference (a) when a LOI is received.

7004. Appealing Unfavorable Determinations. The Personnel Security Appeals Board (PSAB) is the ultimate appellate authority for unfavorable personnel security determinations made by the DON CAF. Individuals wishing to appeal an unfavorable DON CAF determination will adhere to the procedures delineated in reference (a).

CHAPTER 8
CLEARANCES

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	8000	8-2
Citizenship	8001	8-2
Interim Security Clearances	8002	8-3
Denial or Revocation of Security Clearance	8003	8-3
Reestablishing a Security Clearance After a Denial or Revocation	8004	8-4

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CHAPTER 8

CLEARANCES

8000. Basic Policy

1. DON CAF is the single clearance granting authority for the DON. The DON CAF issues final security clearance eligibility for civilian and military personnel, upon affirmation that granting the clearance is clearly consistent with the interests of national security.
2. DON CAF certifies final security clearance eligibility via the Joint Personnel Adjudication System (JPAS). The certification provides commands with the documentation required to support local access determinations. The MCTFS will not be used to provide security clearance certifications for Marines.
3. A security clearance is not authorization for an individual to access classified information; it only indicates that the individual is eligible for access. The decision to grant access to classified information is a separate determination made at the command level dependent on whether an individual who has the requisite security clearance also has a "need-to-know".

8001. Citizenship

1. Only United States citizens are eligible for a security clearance, assignment to sensitive duties, or access to classified information. When compelling reasons exist, in furtherance of the DON mission, including special expertise, a non-U.S. citizen may be assigned to sensitive duties or granted a Limited Access Authorization (LAA) (not a clearance) under special procedures. Reference (a) describes these procedures.
2. Under no circumstances will non-U.S. citizens be granted access to classified information unless CNO (N09N2) has granted a LAA. Granting access to non-U.S. citizens is a security violation involving compromise of CMI, necessitating a Preliminary Inquiry followed by a JAGMAN Investigation and disciplinary action per reference (b).
3. The MAD will verify U.S. citizenship status of first-time clearance candidates and candidates for clearance at a higher level than currently held before beginning security processing, per the conditions outlined in reference (a). U.S. citizens who hold a current, valid security clearance issued by the DON CAF

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

do not have to submit evidence of citizenship to retain clearance at or below the same level.

8002. Temporary Access

1. Temporary access is granted at the command level pending completion of full investigative requirements and pending establishment of security clearance eligibility by the DON CAF.
2. Temporary access is an extraordinary measure, only taken to minimize significant operational impact. It will not be granted for purposes of convenience.
3. Temporary access may be granted provided:
 - a. The individual is a U.S. citizen,
 - b. The individual requires access to classified information in the performance of official duties,
 - c. The appropriate investigation has been initiated, and
 - d. There is no information included on the PSI request or discovered during the LRC that would reflect unfavorably on the individual's loyalty, reliability, or trustworthiness.
4. The Command Security Manager and Assistant Security Manager are delegated the authority to grant temporary access.
5. If the command receives a LOI from the DON CAF to deny an individual's security clearance, any interim security clearance issued will be withdrawn and the associated access will be suspended. Procedures for suspending access are found in reference (a).

8003. Denial or Revocation of Security Clearance

1. Once the DON CAF grants a security clearance it remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months. Whenever information develops via the continuous evaluation program, described in Chapter 10 of this Order, that suggests an individual may no longer be in compliance with personnel security standards, the MAD will report the issues to the DON CAF for adjudication. Reference (a) provides a checklist of issues that must be reported.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

2. If DON CAF determines that an individual either fails or ceases to meet the standards for security clearance, the DON CAF will begin the unfavorable determination process explained in reference (a). If the DON CAF determines a reported issue does not impact on the individual's security clearance, the DON CAF will reissue the security clearance certification.

3. If the DON CAF makes a final unfavorable decision concerning an individual's security clearance, the MAD will remove all accesses authorized, and debrief the individual per reference (a), including execution of a Security Termination Statement.

8004. Reestablishing a Security Clearance After a Denial or Revocation

1. Following an unfavorable security determination by the DON CAF, and after a reasonable passage of time, normally a minimum of 12 months, individuals may submit a request to DON CAF via the Command Security Manager to reestablish their security clearance eligibility. The request must document actions taken to meet the security guidelines set forth in reference (a), and will include a letter of recommendation from the individual's department head. Temporary access or assignment to sensitive civilian positions is not authorized until the DON CAF reestablishes the security clearance.

CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	9000	9-2
Requesting Access	9001	9-2
Local Records Check (LRC)	9002	9-2
Granting Access to Classified Information	9003	9-3
Classified Information Nondisclosure Agreement	9004	9-3
Personal Attestation	9005	9-4
Recording Command Access	9006	9-5
Temporary Access Under Interim Clearance Procedures	9007	9-5
Periodic Reinvestigation Requirements	9008	9-5
Other Special Accesses	9009	9-6
Access by Investigative and Law Enforcement Agents	9010	9-7
Terminating Withdrawing or Adjusting Access	9011	9-7
Suspension of Access for Cause	9012	9-8
Access to Critical Nuclear Weapon Design Information (CNWDI)	9013	9-8

CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

9000. 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. Access to classified information will be based on need to know. Additionally, the level of access authorized will be limited to the minimum level required to perform assigned duties. No one has a right to have access to classified information solely because of rank, position, or security clearance.
3. Limiting access is the responsibility of each individual possessing classified information. Before allowing others access to classified information, individuals possessing classified information must ascertain that the prospective recipient has the required security clearance and the need to know the information to perform official duties.
4. These principles are equally applicable if the prospective recipient is an organizational entity, including commands, other Federal agencies, defense contractors, foreign governments, and others.

9001. Requesting Access. Department heads will request access for civilian and military personnel under their jurisdiction by completing Form 5510/1 (see figure 9-1) and forwarding it to the MAD. This form may be obtained from the Community Planning and Liaison Office and may be locally reproduced. Requests for access will be provided on an individual basis (i.e., one person per request). Personnel requesting access may be subject to screening under the continuous evaluation program prior to their being granted access. See Chapter 10.

9002. Local Records Check (LRC). A LRC is required prior to submitting an investigation request and prior to granting access to classified information to ensure there is no locally available non-adjudicated disqualifying information. A LRC consists of a check of medical, personnel, and PMO records. The MAD will conduct all LRCs.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

9003. Granting Access to Classified Information

1. The Command Security Manager, and Assistant Security Manager are delegated the authority to grant access to classified information to those command personnel, military and civilian, who have an official need to know, an established security clearance, and about whom there is no known unadjudicated disqualifying information. The determination to grant access to classified information is subject to the restrictions contained in reference (a).

2. Access may be granted provided the following requirements have been met:

a. The individual has the appropriate clearance eligibility that will support the access level required, or an investigation/ reinvestigation request has been submitted to the appropriate investigative agency to support a temporary access (also referred to as an interim clearance) or continuing access (see paragraphs 9007 and 9008 herein),

b. The individual must be a U.S. citizen,

c. No disqualifying information is discovered, (if it is, the procedures in paragraph 7002 of this order will apply),

d. The individual has signed a SF 312 Classified Information Nondisclosure Agreement, per paragraph 9004 below.

e. In cases involving Top Secret access or special accesses, the individual has executed an Attestation Statement per paragraph 9005 below.

3. If the individual has the appropriate clearance eligibility, but it is based on an out-of-date investigation, local access may be authorized only after submission of a reinvestigation request to the appropriate investigative agency. Temporary Access (also referred to as interim clearance) procedures are not employed in this situation.

9004. Classified Information Nondisclosure Agreement (SF 312)

1. Per reference (a), a SF 312 must be executed by all persons prior to gaining initial access to classified information. If an individual refuses to sign a SF 312, the individual will not be allowed access to classified information, and the MAD will

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

report the refusal to the DON CAF.

2. The MAD will ensure all military and civilian employees who have not previously executed a SF 312 sign a current SF 312 before being given access. Prior execution of a SF 312 will be considered valid if verified through JPAS.

3. The MAD is authorized to accept the SF 312 on behalf of the U.S. Government.

4. The MAD will forward executed SF 312's as follows:

a. For Marine Corps personnel - Headquarters U.S. Marine Corps (MMSB-20).

b. For Navy personnel - Bureau of Naval Personnel (Pers 312C).

c. For DON civilian employees - HRO, MCAS Yuma for placement in the individual's OPF.

9005. Personal Attestation

1. Per reference (c), prior to being granted access to Top Secret information and/or indoctrinated into a Special Access Program (SAP) or Sensitive Compartmented Information (SCI), individuals will orally attest to understanding their responsibility to protect classified national security information. The statement below will be read aloud and "attested to" in the presence of a witness other than the person administering the brief:

Attestation Statement:

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official need to know. I further understand that, in being granted access to classified information and/or SCI/SAP, a special confidence and trust has been placed in me by the United States Government.

2. The Attestation is required only one time and will be documented in the JPAS.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

9006. Recording Command Access

1. Joint Personnel Adjudication System (JPAS). The MAD will annotate the individual's record in the JPAS database with the access granted, including temporary accesses, special accesses, and other program accesses formally granted (e.g., CNWDI).
2. Department Security Access List (DSAL). Departments holding classified information will maintain a DSAL reflecting individuals granted access to that information. Departments will closely coordinate with the MAD to ensure the accuracy of the list.
3. Access Letters. Once access has been granted, the MAD will endorse figure 9-1 and forward it to the cognizant department. This endorsement will serve as verification of access.

9007. Temporary Access Under Interim Clearance Procedures

1. If the JPAS indicates the individual requires an initial investigation to qualify for a clearance and access, or if the individual has neither the appropriate clearance eligibility nor the required current investigation, the individual may be authorized temporary access under interim clearance procedures once the investigation request has been submitted to the appropriate investigative agency, provided the individual meets all requirements for access noted in paragraph 9003 above.
2. In cases involving interim Top Secret access, the individual must have current final Secret security clearance eligibility, based on a favorable investigation completed within the last ten years, with no break in service exceeding 24 months. See paragraph 8002 of this Order for interim clearance procedures.

9008. Periodic Reinvestigation Requirements

1. Reference (a) requires that access to classified information or assignment to specific duties is to be based on an investigation completed within specific timelines according to the sensitivity of the duties or access level required. Accordingly, personnel whose current investigation has not been completed within the following timelines will not be authorized access to classified information at the level indicated until a reinvestigation request has been submitted to the appropriate investigative agency:

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

a. Access to Top Secret or SCI information - a Periodic Reinvestigation is required every five years.

b. Access to Secret information - a Periodic Reinvestigation is required every ten years.

c. Access to Confidential information - a Periodic Reinvestigation is required every 15 years.

2. PSIs will not normally be requested for any civilian or military personnel who will be retired, resigned, or separated with less than one year service remaining.

3. The MAD will notify the individual six months before the individual's investigation expires of the need to complete and submit a reinvestigation request. If the individual fails to complete and submit the reinvestigation request within that six-month timeframe, the individual's access will be administratively withdrawn or downgraded. Access may be reinstated after the individual completes the reinvestigation request, and it is favorably reviewed and submitted to the appropriate investigative agency:

9009. Other Special Accesses

1. Reference (a) contains procedures and restrictions for granting access to classified information in special circumstances. These special circumstances include:

a. Granting one-time or short duration access at a level higher than that for which the individual is eligible.

b. Granting temporary access to personnel who do not require a security clearance/access to perform regular assigned duties, but require short duration access to attend a classified meeting or training session, or perform annual reserve active duty for training or scheduled inactive duty training.

c. Access by retired personnel.

d. Access for attorneys representing DON personnel.

e. Contractor access.

f. Access authorizations for persons outside the executive branch of the government.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

- g. Access for historical researchers.
- h. Limited Access Authorization for non-U.S. citizens.

90010. Access by Investigative and Law Enforcement Agents.

Investigative agents of other departments or agencies may obtain access to classified information only through coordination with the NCIS. The Security Manager or Assistant Security Manager will be advised of all requests for access to classified information by investigative and law enforcement personnel. In all cases, information will be protected as required by its classification.

90011. Terminating, Withdrawing or Adjusting Access

1. Reference (a) outlines the requirements for terminating, withdrawing, and adjusting clearances and access.
2. Access terminates when an individual transfers from a command. Personnel who are transferring from this command to another will be debriefed per reference (a) and paragraph 4004 of this order.
3. The MAD will administratively withdraw an individual's access when a permanent change in official duties (i.e., MOS changes) eliminates the requirement for security clearance and access. Also, access terminates when an individual separates or retires from the DON or terminates employment. The MAD will debrief the individual per reference (a) and paragraph 4004 of this Order. Execution of a Security Termination Statement is required.
4. The MAD will adjust an individual's access when the level of access required for an individual's official duties changes, provided the new requirement does not exceed the level allowed by the security clearance eligibility. If it does, an appropriate investigation will be requested, and an interim clearance may be granted.
5. The MAD will administratively withdraw or downgrade an individual's access not supported by a current personnel security investigation or reinvestigation. Access may be reinstated after the individual completes a reinvestigation request, and it has been favorably reviewed and submitted to the appropriate investigative agency.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

6. Department Heads will submit requests for the withdrawal or adjustment of access by Station personnel in writing (e-mail acceptable) to the MAD.

7. The administrative withdrawal or downgrading of a security clearance or access is not authorized when prompted by developed derogatory information. If suspension of the individual's access is warranted, it will be accomplished per reference (a).

90012. Suspension of Access for Cause

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the CO may suspend access, per the procedures discussed in paragraph 7002 of this order. Suspension of access for cause may only be used as a temporary measure, which must be resolved through either a favorable or unfavorable security determination by the DON CAF prior to the individual being transferred to a different command.

2. Suspension of access is required when a civilian employee is incarcerated as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

3. Suspension of access is required when a military member is discharged under Other Than Honorable conditions, is incarcerated as the result of a conviction for a criminal offense or violations of the Uniform Code of Military Justice (UCMJ), is declared a deserter, or is absent without leave for a period exceeding 30 days.

4. When a determination is made to suspend access to classified information, the procedures set forth in reference (a) will be followed.

90013. Access to Critical Nuclear Weapon Design Information (CNWDI)

1. Access to and dissemination of CNWDI is of particular concern due to the extreme sensitivity of this type of information. Access must be limited to the absolute minimum number of persons needed to meet mission requirements.

2. The MAD is responsible for processing requests for CNWDI access, and will execute the following procedures, as set forth

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

in reference (a):

a. Ensure personnel authorized access to CNWDI have a final Top Secret or final Secret clearance (as appropriate).

b. Verify the "need to know" by personnel requesting CNWDI access, and prepare access authorization letters.

c. Brief personnel requiring access to CWDI on its sensitivity. Record the access authorization in JPAS, and maintain briefings and access authorizations in appropriate security records.

d. Debrief personnel upon termination of CNWDI access due to transfer, reassignment, etc. Maintain debriefing records for two years after access is terminated.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

INSERT MCASY FORM 5510/1
HERE

Figure 9-1. Sample MCASY FORM 5510/1, "Request for Access to Classified Military Information (CMI) and Local Records Check."

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

personnel to programs designed to counsel and assist them when they are experiencing financial, medical, or emotional difficulties.

2. Keys to an effective continuous evaluation program are security education and positive reinforcement of reporting requirements in the form of management support, confidentiality, and employee assistance referrals.

10002. Program Elements

1. Security Education. The Security Education Program is discussed in Chapter 4 of this order. Indoctrination and orientation training and annual security refresher briefings will emphasize the security standards required of all personnel who access classified information, and the avenues open to personnel should they require assistance or otherwise have difficulty or concerns in maintaining trustworthiness standards.

2. Employees Education and Assistance Program. There are various programs available on the Station through the Marine Corps Community Services (MCCS) for personnel who have questions or concerns about financial matters, mental health, or substance abuse. The goal is to assist individuals while there is still a reasonable chance of precluding a long-term employment or security clearance-related issue.

3. Performance Evaluation System. Per reference (a), the Command Security Manager, Assistant Security Manger, Secondary Control Point Custodians, and all other personnel whose duties significantly involve the handling or management of classified information will be rated on their management of classified information during annual performance rating cycles. In addition, supervisors will comment on the continued security clearance eligibility of subordinates who have access to classified information in conjunction with regularly scheduled performance appraisals.

10003. Command Reports of Locally Developed Unfavorable Information

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties, the MAD will report that information to the DON CAF, per reference (a). The following circumstances will be reported, without attempting to apply or consider any mitigating factors that may

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

exist:

a. Involvement in activities which, or sympathetic association with persons who, unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.

b. Foreign influence concerns or close personal association with foreign nationals or countries.

c. Foreign citizenship (dual citizenship) or foreign monetary interests.

d. Sexual behavior that is criminal or reflects a lack of judgment or discretion.

e. Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security processing requirements.

f. Unexplained affluence or excessive indebtedness.

g. Alcohol abuse.

h. Illegal or improper drug use/involvement.

i. Apparent mental, emotional or personality disorder(s).

j. Criminal conduct.

k. Noncompliance with security requirements.

l. Engagement in outside activities which could cause a conflict of interest.

m. Misuse of Information Technology Systems.

2. If circumstances warrant, the individual's access to classified information will be suspended for cause. The suspension action will be accomplished per reference (a).

3. Once clearance eligibility is suspended, the individual may not be granted access until the DON CAF has reestablished clearance eligibility.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

4. In cases where unfavorable information has been resolved by local investigation or inquiry, the MAD will notify the DON CAF of the inquiry results. Temporary clearance eligibility may be requested, and authorized by DON CAF if the local inquiry developed the necessary mitigation and there are no other unresolved security issues or other related pending inquiries or investigation.

5. Whenever military personnel are listed on the MCAS Yuma PMO Blotter which indicates their involvement in unfavorable activities as described in paragraph 10003, the MAD is required to report such activities to DON CAF. Close coordination between MAD and H&HS is required to track these submissions and submit follow up reports as required.

CHAPTER 11
VISITOR CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	11000	11-2
Classified Visit Request Procedures	11001	11-2
Classified Visits to MCAS Yuma	11002	11-3
Visits by Foreign Nationals and Representatives of Foreign Entities	11003	11-4

CHAPTER 11

VISITOR CONTROL

11000. Basic Policy

1. For security purposes, the term visitor means:

a. A visitor to MCAS Yuma is any person who is not attached to or employed by this Command.

b. Individuals assigned to temporary additional duty (TAD) to MCAS Yuma. Personnel on temporary duty orders, reservists on active duty for training, or those personnel assigned on a quota to a school or course of instruction are considered as visitors when not attached to this Command.

c. Cleared DoD contractors assigned to MCAS Yuma who occupy or share government spaces for a predetermined period.

2. Only visitors with an appropriate level of security clearance and need to know will be granted access to classified information.

3. The movement of all visitors will be controlled to protect classified information. When escorts are used, they must ensure visitors have access only to information they have been authorized to receive.

4. Any visitor expressing unusual interest in information they are not authorized to receive, or expressing feelings inimical to the best interests of the U.S. will be reported to the Command Security Manager.

5. Visits by the general public are permitted on an unclassified basis only. This includes group tours arranged through the Joint Public Affairs Office as well as open house or special occasions where the general public has been invited aboard the Station.

11001. Classified Visit Request Procedures

1. MCAS Yuma personnel will inform the MAD if they will require access to classified information during visits to other commands or activities for meetings, TAD, or other reasons. The following information is required for completion of the visit

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

or restrictions with the applicable point of contact.

2. A formal visit request is not required for employees of the executive branch who are U.S. citizens when there is an established working relationship and the clearance level and bounds of need to know of the government employee visiting are known.

3. Occasionally, visitors will arrive without previous notification or advance passing of the security clearance. In such cases, the visitor will not be granted access to classified information until a visitor request is received and properly vetted.

4. All departments will establish procedures for visits to their area(s), including maintenance of a visitor record, if deemed necessary, and any areas "off - limits" or requiring cleared escorts. Cleared escorts will accompany visitors to all restricted areas and areas containing classified or sensitive but unclassified (SBU) information.

5. Any visitor who is to be authorized access to classified information must present adequate identification at the time of the visit. The identification media will be verified against the information contained in the visit request. If the picture does not look like the person, do not accept the ID. Report any attempt to gain access to classified information by persons using fraudulent ID'S to the Command Security Manager or to the NCIS.

6. Procedures for classified visits by members of Congress and classified visits by representatives of the General Accountability Office (GAO) are described in reference (a).

11003. Visits by Foreign Nationals and Representatives of Foreign Entities. Reference (g) provides guidance on visits by foreign nationals and representatives of foreign entities.

CHAPTER 12

CLASSIFICATION MANAGEMENT

12000. Basic Policy. Executive Order 12958 is the only basis for classifying National Security Information, except as provided by the Atomic Energy Act of 1954, as amended. DON policy is 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.

12001. Classification Levels. Information that requires protection against unauthorized disclosure in the interest of national security must receive one of three classification designations: Top Secret, Secret, or Confidential. Terms such as "For Official Use Only", "Law Enforcement Sensitive", or "Secret Sensitive" (SS), are not security classifications and will not be used to identify U.S. classified information.

12002. Classification Determination. When drafted, classified material receives either an original classification or derivative classification determination.

1. Original Classification. Original classification is based on the initial decision that an item of information might cause damage to national security if subjected to unauthorized disclosure. Only Original Classification Authorities (OCAs) can make this decision. OCAs have been trained in the exercise of this authority and have program responsibility or cognizance over the information. No official at MCAS Yuma has original classification authority.

2. Derivative Classification. Derivative classification may be accomplished by anyone who incorporates, paraphrases, restates, or generates, in new form, information that is already classified. It involves marking newly developed information based on classified source documents or classification guidance. It is not the mere duplication or reproduction of existing classified information. Derivative classifiers will:

a. Observe and respect the original classification determinations made by OCAs (as codified in classified source documents and security classification guides).

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

b. Use caution when paraphrasing or restating information extracted from a classified source document(s) to determine whether the classification may have been changed in the process.

c. Carry forward to any newly created information, any applicable classification markings.

CHAPTER 13

MARKING

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	13000	13-2
Marking Classified Files, Folders and Groups of Documents	13001	13-2
Marking Removable Automated Information System (AIS) Storage Media	13002	13-3
Marking E-Mail Transmitted on the Secret Internet Protocol Router Network (SIPRNET)	13003	13-3

CHAPTER 13

MARKING

13000. Basic Policy

1. All classified information will be clearly marked with the date and office of origin, the appropriate classification level, and all required "associated markings" (see reference (b) for exceptions to this policy). "Associated markings" include those markings that identify the source of classification; downgrading and declassification instructions; and warning notices, intelligence control markings and other miscellaneous markings (see reference (b) for guidance on the placement of associated markings).

2. The proper marking of a classified document is the specific responsibility of the original or derivative classifier. The purpose of marking classified material is to alert the user that classified information is contained in a document and they also serve to warn users of special access, control or safeguarding requirement and to assist in extracting, paraphrasing, downgrading, and declassifying actions.

3. 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.

4. Classified material will be physically marked, annotated, or identified per reference (b). The MAD will provide assistance as needed.

13001. Marking Classified Files, Folders and Groups of Documents

1. When a file, folder, or group of classified documents is removed from secure storage, it must be conspicuously marked with the highest classification of any classified document it contains, with an appropriate classified document cover sheet attached.

2. The only document cover sheets authorized for use at MCAS Yuma are as follows:

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

- a. Top Secret Cover Sheet, SF 703.
- b. Secret Cover Sheet, SF 704.
- c. Confidential Cover Sheet, SF 705.

13002. Marking Removable Automated Information System (AIS) Storage Media

1. Personnel will mark removable AIS media and devices with the appropriate color-coded label that indicates clearly the highest overall classification level and associated markings of the information they contain, per the following:

- a. Sensitive Unclassified - SF 710 (Green).
- b. Confidential - SF 708 (Blue).
- c. Secret - SF 707 (Red).
- d. Top Secret - SF 706 (Orange).

2. Removable AIS media and devices that store information recorded in the analog or digital form include magnetic tape reels, cartridges, cassettes, removable hard drives, CD ROM disks, DVD disks, disk cartridges, disk packs, diskettes, thumb drives, and magnetic cards. See reference (b) for placement instructions.

13003. Marking E-Mail Transmitted on the Secret Internet Protocol Router Network (SIPRNET)

1. Originators of e-mail containing Secret or Confidential information sent over the SIPRNET will apply classification markings in the same manner as any other hard copy classified document, per Chapter 6 of reference (b).

a. The subject and all portions and paragraphs will contain applicable security classification markings, (U), (C), or (S), plus any applicable intelligence control markings.

b. There will be a "Derived From:" and "Declassify On" marking.

c. There will also be overall page markings indicating the highest classification (Confidential or Secret) of the e-mail, plus any applicable intelligence control markings, applied

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

center top and bottom of each page of the e-mail in text larger than the text of the e-mail itself. Although not required, highlighting the page markings in bold blue or red is encouraged.

2. Unlike Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) e-mail, which is always unclassified, unclassified SIPRNET e-mail must be plainly marked as "unclassified" prior to sending, printing, or downloading.

3. If clarification is required on the overall classification of SIPRNET e-mail, and especially on any missing portion markings, the originator is the only authority that can clearly identify and mark/re-mark any questionable information.

CHAPTER 14
SAFEGUARDING

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	14000	14-2
Responsibility	14001	14-2
Control Measures	14002	14-3
Classified Messages	14003	14-3
SIPRNET E-Mail and Other Electronically Transmitted Material	14004	14-3
Working Papers	14005	14-3
Special Types of Classified and Controlled Unclassified Information	14006	14-4
Processing Classified Information on Information Systems	14007	14-5
Care During Working Hours	14008	14-6
End-of-Day Security Checks	14009	14-7
Safeguarding During Visits	140010	14-8
Safeguarding During Classified Meetings	140011	14-8
Reproduction of Classified Material	140012	14-9

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

- a. Dated when created.
- b. Conspicuously marked, centered top and bottom on each page, with the highest classification level of any information they contain along with the words "Working Paper."
- c. Protected per the assigned security classification level.
- d. Destroyed, by authorized means, when no longer needed.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

CHAPTER 14

SAFEGUARDING

14000. Basic Policy

1. Classified material will be processed only in secure facilities, on accredited AISSs, and under conditions that prevent unauthorized individuals from gaining access to it. The CMCC and all SCPs within this command will be designated, in writing, as restricted areas per MCO P5530.14, Marine Corps Physical Security Program Manual. Signs designating these areas as restricted areas will be posted on or near the access door.

2. Classified information is the property of the U.S. Government and not personal property. This includes classified notes from a training course or conference. Classified material is official information that must be safeguarded, transmitted and destroyed per this order and reference (b). When individuals transfer from this command, their classified notes may be officially transferred to their new command. When the individual is separated, released or retired from the DON, all classified material must be turned in to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers.

14001. Responsibility

1. Anyone who has possession of classified material is responsible for safeguarding it at all times, and particularly for locking classified material in an appropriate security container whenever it is not in use or under direct supervision of authorized persons. The custodian must follow appropriate procedures to ensure 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

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

the general public. LES information should not be released to the media. LES information will be protected from unauthorized disclosure and disposed of by shredding.

14007. Processing Classified Information on Information Systems. The following control measures for classified processing will be followed at this command:

1. Control and Accountability Measures

a. Classified removable media will be controlled and safeguarded as required for the highest classification of data that they contain.

b. Removable magnetic media, such as removable hard disks, bubble memory boards, etc., will be labeled with a color-coded sticker per paragraph 13002 of this Order. They will also be affixed with a Data Descriptor label (SF 711) indicating the classification level; control number, when assigned; dissemination control information, if applicable; and the originator.

c. All classified media will be stored in GSA approved security containers when not in use.

d. Systems with internal hard disks must be protected and physically secured at all times at the level afforded the highest classification of data ever processed on the system. If the facility is not approved for open storage of classified information, the system must be secured in a safe or vault whenever not attended by cleared, authorized persons.

e. When disposing of media, follow any special procedures as they relate to the specific media involved. Destruction procedures are set forth in reference (b), and Chapter 16 of this Order.

2. Physical and Personnel Measures

a. Only those individuals possessing the requisite security clearance and access for the highest classification of data in the system, and possessing the need to know for any of the information accessible through the system, will be allowed access to the system.

b. All personnel entering secure areas to perform maintenance on computers used for classified processing must

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

have an appropriate security clearance and access to the highest classification of data in the system.

3. System Security Measures

a. Systems must be afforded that level of protection required by the highest classification of data processed by the system.

b. Classified information will only be processed on U.S. Government equipment, in secured workspaces, and handled by authorized, cleared personnel. Privately owned systems are not authorized to process classified information. Additionally, privately owned software or public domain software from nongovernmental sources is not authorized to process classified information.

14008. Care During Working Hours

1. When classified documents are removed from storage for working purposes, an appropriately cleared person must keep them under surveillance at all times. They must be kept face down when not in use or covered with an appropriate cover sheet. SF 703 (Top Secret), SF 704 (Secret) and SF 705 (Confidential) will be used for this purpose. Classified material WILL NEVER be left unattended.

2. Protect preliminary drafts, plates, stencils, stenographic notes, worksheets, computer printer and typewriter ribbons, computer storage media, and other classified items according to their security classification level. Immediately destroy these items after they have served their purpose.

3. Do not discuss classified information with or in the presence of unauthorized persons. All office spaces where classified information 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. Practice the need to know principle.

4. In a mixed working environment (i.e., classified and unclassified), AIS media used for processing or storing classified information will be marked with the appropriate SF label (SF 706, 707, 708, 709, 710, or 711, as applicable.) In a totally unclassified working environment, SF labels are not

required.

5. Personal Electronic Devices (PEDs) are prohibited in vaults, secure rooms, or other areas where classified information is processed, stored, or discussed, and will be subject to confiscation. This restriction includes Personal Digital Assistants (PDAs), Palmtops, hand-held computers, cell phones, two way pagers, wireless e-mail devices, and audio and video recording devices capable of recording, copying, storing or transmitting. Electronic equipment that is confiscated will be evaluated to determine if it contains any classified or SBU information. Devices determined not to contain any classified or SBU information will be returned to the owner. If classified information is found on the electronic device, the Command Security Manager/Assistant Security Manager will be notified. Per Chapter 18 of this Manual, a Preliminary Inquiry will be initiated. The device will be degaussed or destroyed at the discretion of the Security Manager, and the owner will be subject to administrative and/or disciplinary action.

14009. End-of-Day Security Checks

1. All custodians of classified information will conduct security checks at the end of normal working hours to ensure that all areas which process classified information are properly secured. The SF 701, Activity Security Checklist, will be used for this purpose. A single SF 701 may be employed for interconnected office spaces. Custodians will post the SF 701 near the main entrance door.

2. Those conducting security checks will ensure that:

a. Security containers have been locked. The Security Container Check Sheet, SF 702, will be used as the opening and locking record for all security containers, vaults, and secure rooms. Appropriate entries will be made on the SF 702 each time a container or vault/secure room is opened and locked. A person, when available, other than the person locking the container, will also annotate the check sheet at the end of normal working hours as a double check.

b. The contents of desks, wastebaskets and other surfaces and receptacles containing classified material have been properly stored or destroyed.

c. Windows and doors have been locked.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

d. All classified material is stored in the manner prescribed and that burn bags, if used, are properly stored or destroyed.

e. If applicable, security alarms and equipment have been activated.

f. Check other items as directed (i.e., STE phones, computers, copiers etc.).

140010. Safeguarding During Visits. Only visitors with an appropriate clearance level and need to know will be granted access to classified information. Refer to reference (b) and Chapter 11 of this Order for visit procedures.

140011. Safeguarding During Classified Meetings

1. Classified information will not be disclosed at conferences, seminars, exhibits, symposia, training courses, or other gatherings (hereafter called meetings) unless disclosure of the information serves a specific U.S. Government purpose and adequate security measures are taken to control access to the information and prevent its compromise.

2. Meetings in which classified information will be disclosed must be approved in advance by the Command Security Manager.

3. A meeting conducted or sponsored by any departmental staff section onboard the Station in which classified information will be disclosed must be held at a cleared facility and only after determining that:

a. Disclosure of classified information at a meeting is in the best interest of national security.

b. The use of conventional channels for dissemination of classified information will not accomplish the purpose of the meeting.

c. The location selected facilitates proper control and dissemination of classified information, including secure storage. Technical Surveillance Countermeasures (TSCM) support will be requested per SECNAVINST 3850.4, Technical Surveillance Countermeasures Program.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

d. Adequate security measures and access procedures will be imposed.

e. Each person attending has been authorized access to information of equal or higher classification than the information being disclosed.

f. Admittance is limited to those on an approved access list and then only upon proper identification.

g. Provisions are made to control and safeguard classified material given to those attending and to retrieve the material or effect transfer of control through approved methods.

h. Sessions are monitored to ensure discussions are limited to the level authorized.

i. Classified notes received or taken or electronic recordings will be controlled per chapter 14 of this Order.

4. The department/section conducting a classified meeting is responsible for ensuring that visit requests for attendees are on file prior to conducting the meeting. The department point of contact will coordinate with the MAD to verify classified material access eligibility of attendees.

5. When it becomes necessary to provide temporary storage of classified material brought aboard MCAS Yuma after normal working hours, the METOC will serve as the overnight repository for classified material (up to the Secret level) hand-carried by visitors from other commands. If brought aboard MCAS Yuma during normal working hours, classified material may be stored in the CMCC.

6. Further restrictions and requirements concerning classified meetings are contained in reference (b).

140012. Reproduction of Classified Material

1. Basic Policy

a. Classified information will be reproduced only when it is considered mission-essential. Any reproduction limitations placed on classified material by originators and special controls applicable to special types of classified information will be adhered to.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

b. The following controls on reproduction of classified material apply not only to traditional documents, but also to AIS storage media, films and videotapes, recordings, microfilms, photographs, slides, and many other formats.

2. Controls on Reproduction

a. The convenience of reproduction equipment will not preclude obtaining proper authorization needed for reproducing classified material.

(1) Individuals desiring to reproduce Secret and below material will obtain authorization from the Command Security Manager or Assistant Security Manager. Figure 14-1 will be used. This form may be locally reproduced.

(2) Confidential material may be reproduced in departmental spaces after inspection and approval of their reproduction equipment by the Command Security Manager/Assistant Security Manager.

b. Reproduced copies of classified documents will be afforded the same security controls as those required for the original documents. Personnel will ensure all classified markings are present and visible on the reproduced material. The individual reproducing the material will remark reproduced material on which classification markings are illegible.

c. Any samples, waste, or overruns resulting from the reproduction process will be safeguarded according to the classification of the information involved. This material will be promptly destroyed as classified waste.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

REQUEST FOR REPRODUCTION OF CLASSIFIED MATERIAL		
SECTION I (REQUEST)		
To: Security Manager, MCAS Yuma	From: (Department)	Date
Classification of Material (Check One) <input type="checkbox"/> Secret <input type="checkbox"/> Confidential	Originator	Date of Material
Subject or Title of Material		
Control No. (If Applicable)	No. of Copies Required	Required by Date
Justification		
Distribution (If Applicable)		
Point of Contact/Phone Number		
Printed Name of Department Head	Department Head Signature	
SECTION II (APPROVAL/DISAPPROVAL)		
From: Security Manager, MCAS Yuma	To: (Department)	Date
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved Reason for Disapproval		
Signature of Approving Official	Title	

Figure 14-1. Sample Reproduction/Distribution request

CHAPTER 15

DISSEMINATION, TRANSMISSION AND TRANSPORTATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	15000	15-2
Prepublication Review	15001	15-2
Dissemination to DOD Contractors	15002	15-2
Dissemination to Foreign Governments	15003	15-3
Mailing Classified Material	15004	15-3
Telephone Transmission	15005	15-3
Receipt for Classified Information	15006	15-3
Hand Carrying Classified Information	15007	15-3
Authorization to Hand Carry Classified Information in a Travel Status	15008	15-4

CHAPTER 15

DISSEMINATION, TRANSMISSION AND TRANSPORTATION

15000. Basic Policy

1. Classified and controlled unclassified information originated or received by this command will be disseminated only to those activities having a need to know, subject to any restrictions imposed by originators or higher authority.
2. Restraints on the dissemination of special access program information, controlled unclassified information (e.g., FOUO), and technical documents are contained in reference (b).
3. Only appropriately cleared personnel or carriers will transmit, transport, escort, or hand carry classified information, per the provisions of reference (b).
4. Unless a specific kind of transmission or transportation is restricted, the means selected will minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.

15001. Prepublication Review. Material prepared for public release will not contain classified material or prescribed technical data. MCO 5510.9B, Security of Information for Public Release, identifies certain categories of Marine Corps information that must be submitted for a security review by the Commandant of the Marine Corps (Code CIC) before being released to the public, including information intended for placement on the command web site accessible through the INTERNET. In order to prevent the inadvertent disclosure of classified information, the Public Affairs Officer will coordinate with the MAD on the release of all official Marine Corps information that may have national security implications.

15002. Dissemination to DOD Contractors. Before disclosing any classified information to a DOD contractor, departments and staff sections must determine that the contractor has a current security clearance equal to or higher than the level of classified information to be disclosed. This is accomplished using the contracting facility's certification of security clearance provided on the classified visit request (see chapter 11 of this Order), which will be provided to the MAD.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

15003. Dissemination to Foreign Governments. Authority for disclosure of classified information to foreign governments has been centralized in the Foreign Liaison Office, HQMC and must be authorized in writing. Foreign visit requests received from the FLO, and approvals/disapprovals to disclose classified information will be processed via the MAD.

15004. Mailing Classified Material. All classified material to be mailed to another activity will be brought to the MAD. No classified material may be mailed directly from a SCP to another activity. This includes documents to be transferred to other commands on the Station for retention by those commands. The CMCC will prepare the classified material for mailing, following the procedures in Chapter 9 of reference (b).

15005. Telephone Transmission. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits. Unless special equipment is being used, there is no reason to believe a line is secure. DD Form 2056 decals will be placed on all official telephones (except for STU-III's and STE's) to alert users not to discuss classified information and that the telephone is subject to monitoring at all times.

15006. Receipt for Classified Information. Acknowledgement of receipt is required when transmitting or transporting Secret information in and out of the command, and for all classified information provided to a foreign government or its representatives. OPNAV 5511/10, Record of Receipt, or a locally prepared form will be used. Receipts will contain only unclassified information that clearly identifies the information being transmitted. The receipt must be signed and returned to the MAD regardless of the method of transmission. Receipts will be maintained for two years.

15007. Hand Carrying Classified Information

1. No one is authorized to hand carry classified information without the authorization of the Security Manager or Assistant Security Manager. This authorization must be in writing, using a DD 2501, Courier Authorization Card, or a courier authorization letter.

2. Personnel will take all reasonable precautions while hand carrying classified information to prevent inadvertent disclosure.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

a. Use a cover sheet or file folder when hand carrying classified information within a building, or between buildings onboard MCAS Yuma.

b. If the material is to be transported outside the confines of MCAS Yuma, it will be double-wrapped. A locked briefcase may serve as the outer cover, except when hand carrying aboard commercial aircraft.

3. When classified information is hand carried to another command, the same requirements for mailing classified material (e.g., wrapping, addressing, receipts, etc.) to another command also pertain.

4. Classified material will not be carried into public places such as the exchange, snack bars, barbershop, etc. Under no circumstances are couriers to take classified material to their quarters, either aboard the Station or off.

5. The DD 2501 will be issued to those personnel who have a recurrent need to escort or hand carry classified information either as part of normal duties or in an official travel status. The expiration date on the DD 2501 may not exceed three years from the issue date. The DD 2501 will be retrieved upon an individual's transfer, termination of employment, or when authorization is no longer required. The DD 2501 is controlled and issued by the MAD and local reproduction is prohibited.

6. All personnel hand carrying classified information between the MAD and a SCF are required to have a DD 2501 in their possession.

7. The DD 2501 may be used between DOD commands worldwide and provides sufficient authorization to hand carry classified information aboard a U.S. military aircraft. It does not provide sufficient authorization to hand carry classified information aboard commercial aircraft, in which case a courier authorization letter must also be carried by the traveler.

15008. Authorization to Hand Carry Classified Information in a Travel Status

1. Because of the security risks inherent in hand carrying classified material while in a travel status, this practice is not authorized except under extraordinary or emergency circumstances. The widespread use of the SIPRNET makes the need to hand carry classified information while in a travel status

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

almost obsolete. Hand carrying classified information in a travel status will only be authorized under those circumstances described in reference (b).

2. Requests to hand carry classified material aboard commercial passenger aircraft will be submitted in writing to the Command Security Manager, and will contain the information listed in reference (b). Upon receipt of the request and the material to be transported, the MAD will prepare a courier authorization letter. The designated courier will then personally receipt for the authorization at the MAD office and receive a briefing on their security responsibilities.

3. All individuals authorized to hand carry classified information while in a travel status will acknowledge their security responsibilities by reading and signing a briefing form, figure 15-1, prior to departure from the command. A copy of the signed briefing form will be maintained by the MAD.

4. For additional guidance pertaining to escorting or hand carrying classified information aboard commercial passenger aircraft, refer to reference (b).

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

STATEMENT OF UNDERSTANDING FOR ESCORTING OR HANDCARRYING
CLASSIFIED INFORMATION

I, _____ (Grade, Name, SSN (last 4 only)/MOS) _____, hereby certify that I have read and understand my security responsibilities listed below while escorting or hand carrying classified information. I understand that I have the responsibility to safeguard and protect that information at all times to prevent loss or compromise. I further understand that in the event of unforeseeable circumstances (e.g., injury or accident) that may incapacitate me or otherwise impair the direct control and safeguarding of classified material in my charge, all efforts will be made to contact the MCAS Yuma Security Manager at _____ (telephone number). I will at that time provide information as to the nature of the problem, my location, and the disposition of the classified material.

I acknowledge the following:

1. I am liable and responsible for the information being escorted.
2. The information is not, under any circumstances, to be left unattended.
3. During overnight stops, classified information will be stored at a U.S. embassy, military base or appropriately cleared DOD contractor facility and will not, under any circumstances, be stored in vehicles, hotel rooms or safes. When I surrender any package containing classified material for temporary storage, I will obtain a receipt signed by an authorized representative of the U. S. embassy, facility or installation accepting responsibility for safeguarding the package.
4. The information will not be opened enroute except in the circumstances described below:
 - a. There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights. Carry-on bags and packages may be subjected to X-raying and inspection by customs or airline/airport security officials.

Figure 15-1. Statement of Understanding of Escorting or Hand Carrying Classified Information

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

b. If there is a question about the contents of the package, I will present the courier authorization to the official or to the official's supervisor, if necessary. If the official demands to see the actual contents of the package, it may be opened in his or her presence, in an area out of sight of the general public. However, under no circumstances will classified information be disclosed. Immediately after the examination, I will request that the package be resealed and signed by the official to confirm that the package was opened.

c. I will inform both the addressee and the MCAS Yuma Security Manager and Assistant Security Manager in writing of the opening of the package.

5. The information will not be discussed or disclosed in any public place or conveyance.

6. I will not deviate from the authorized travel schedule.

7. I am responsible for ensuring that personal travel documentation {passport, courier authorization, and medical documents) are complete, valid, and current.

8. I will carry a copy of an inventory of the contents in the sealed package and submit a copy to the MCAS Yuma Security Manager or Assistant Security Manager for retention.

9. Upon return, I will return all classified information in a sealed package or furnish documentation signed by an authorized security official of the addressee organization for any information that is not returned.

Signature of Courier

Date Signed

Copy to:
Security Manager
MAD

Figure 15-1. Statement of Understanding of Escorting or Hand Carrying Classified Information

CHAPTER 16

STORAGE AND DESTRUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	16000	16-2
Storage Requirements	16001	16-2
Establishment of Classified Storage Areas	16002	16-3
Combinations	16003	16-4
Destruction of Classified Information	16004	16-5
Destruction Methods	16005	16-6
Destruction Procedures	16006	16-6
Destruction of Unclassified Material	16007	16-7

CHAPTER 16

16-1

STORAGE AND DESTRUCTION

16000. Basic Policy

1. All classified information that is not being used or not under the personal observation of cleared persons who are authorized access will be stored in the manner prescribed by reference (b). To the extent possible, areas in which classified information is stored will be limited.

2. Weapons or sensitive items, such as money, jewels, precious metals, or narcotics will not be stored in the same security containers used to store classified information.

3. There will be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction will not be marked or posted on the security container. This does not preclude the placing of required decals and necessary information for other purposes.

4. SCP Custodians will report any weakness, deficiency, or vulnerability in equipment being used to store classified information to the MAD. Reports must fully describe the weakness, deficiency, or vulnerability, how it was discovered, and the measures taken to mitigate it.

16001. Storage Requirements

1. All classified information not under the personal control or observation of an appropriately cleared person will be stored in a locked General Services Administration (GSA) approved security container, vault, or secure room per the storage requirements in reference (b).

2. All security containers, vaults, and secure rooms will be equipped with locks meeting Federal Specification FF-L-2740 (i.e., the Mas-Hamilton X-07, X-08, or X-09).

3. Authorization to store classified material in any office space will be requested from the Command Security Manager (see paragraph 16002 below for procedures on establishing authorized classified storage areas). A Physical Security Evaluation (PSE)

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

will be conducted by the Provost Marshal's physical security section, to determine the degree of security afforded by the existing area, and to recommend additional security requirements when necessary. No storage of classified information is authorized without this survey.

4. New security storage equipment will not be procured until:

a. The MAD has been consulted.

b. A PSE of existing equipment and a review of classified records on hand have been completed.

c. It has been determined that it would not be feasible to use available equipment or to retire, return, declassify, or destroy a sufficient volume of records currently on hand to make the needed security storage space available.

d. The Command Assistant Security Manager will be kept informed of all changes in location, removal or retirement of security containers used for storing classified information.

5. Entrances to vaults or secure rooms will be under visual control during duty hours to prevent entry by unauthorized personnel, or equipped with electric, mechanical, or electromechanical access control devices to limit access. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford by themselves the required degree of protection for classified information and will not be used as a substitute for the locks required by Federal Specification FF-L-2740. Existing mechanical combination locks may not be repaired, but will be replaced with locks meeting Federal Specification FF-L-2740, as per reference (b).

16002. Establishment of Classified Storage Areas

1. All classified information received or originated within the command will be stored in authorized command areas only. The command authorized storage areas will afford the security measures necessary to prevent unauthorized persons from gaining access to classified information.

2. The Command CMCC is the primary storage area for classified material addressed to or originated by this command. SCPs are classified storage areas at department levels established to facilitate daily access by cognizant personnel. SCPs will be inspected and authorized in writing by the Command Security

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

Manager prior to the storage of classified information within the department.

3. To establish a SCP, the following items must be completed:

a. The applicable department head will submit a request for the establishment of a SCP to the Command Security Manager, with a copy to the MAD. The request will contain complete justification for establishing the SCP as an operational requirement vice a convenience. Additionally, the letter of request will identify the amount and classification level of information to be stored.

b. A physical security survey/evaluation will be conducted by the Provost Marshal's physical security section on the proposed SCP. The physical security survey/evaluation will determine if adequate controls are present to provide protection for the classified information to be stored.

c. The applicable department head will appoint a primary and alternate SCP in writing for the proposed SCP (see Figure 2-4). A copy of the appointment letters will be forwarded to the MAD.

4. After all the requirements listed above have been completed satisfactorily, the Command Security Manager will designate the proposed SCP as an authorized command classified storage area (see Figure 16-1).

5. Newly appointed SCP custodians and alternate custodians will ensure they complete the indoctrination training for newly appointed custodians within three months following the establishment of the SCP (see paragraph 4003 of this order).

16003. Combinations

1. Only trained personnel will change combinations. A lockout, as a result of an untrained individual attempting to change a combination, could result in administrative and/or disciplinary action. To prevent a lockout, two individuals should try the combination before closing the container or vault door.

2. Only personnel who have the responsibility and possess the appropriate security clearance will change combinations to security containers, vaults, or secure rooms. Combinations will be changed as follows:

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

- a. When first placed in use.
 - b. When an individual knowing the combination no longer needs access to it, unless other sufficient controls exist to prevent access to the lock.
 - c. When a combination has been subjected to compromise.
 - d. When taken out of service, built-in combination locks will then be reset to the standard combination 50-25-50.
3. The combination of a container, vault, or secure room used for the storage of classified information is classified at the same level as that of the highest category of the information stored within. Any written record of the combination will be marked with the appropriate classification level.
4. Custodians will record combinations using a SF 700 "Security Container Information."
- a. The SF 700 will contain the location of the security container, vault, or secure room, and the names, home addresses, and home telephone numbers of all persons having knowledge of the combination. If necessary, continue the listing of persons having knowledge of the combination on an attached sheet.
 - b. Custodians will post Part 1 of the SF 700 on an interior location of all security containers, vaults, and secure room doors. If a container is found unsecured, unattended, or shows evidence of attempted unauthorized entry, the appropriate official can then be notified.
 - c. Custodians will mark the appropriate classification level on Parts 2 and 2A of the SF 700, and seal the combination within the SF 700 envelope. SCP combinations will be stored at the Command CMCC, and CMCC combinations will be stored at the Station METOC SCP, to allow for emergency access during non-working hours.

16004. Destruction of Classified Information

1. Classified material holdings will be kept to the minimum required for mission accomplishment. Destroy classified and controlled unclassified information when no longer needed for operational purposes.

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

2. Destruction of classified material will be accomplished per reference (b).
3. SCP Custodians will hold an annual "clean-out" day to focus on disposition of unneeded classified information.
4. COMSEC information will be destroyed per EKMS-1. AIS storage media will be declassified or destroyed per Don IA Pub P-5239-26, Remanence Security Guidebook.
5. Classified information that cannot be destroyed will be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center. SCPs shall submit a quarterly report showing all accountable material to include copies of destruction records.

16005. Destruction Methods

1. Cross-cut shredders used to destroy classified information must be able to reduce the material to shreds no greater than five (5) square millimeters. Strip shredders will not be used for destruction of classified information.
2. The Command Security Manager/Assistant Security Manager will ensure all destruction equipment to be used for destroying classified information meet or exceed the above requirements.
3. Diskettes will be shredded using a crosscut shredder.
4. MAD maintains a CD-ROM destroyer located in the vault. SCP's may schedule use of these assets for destruction; however, SCP's are responsible for remnant disposal.
5. The use of "overwrite" software for the purpose of declassifying magnetic storage media as a method of destruction is strictly prohibited. Magnetic storage media will be shipped to the National Security Agency for disposal.

16006. Destruction Procedures

1. All witnesses to the destruction of classified material will possess a security clearance and access equal to the highest classification of the material being destroyed.
2. When destruction of Secret and Confidential information is conducted at an authorized SCP, the SCP Custodian will record the destruction and submit a copy to MAD for accountability

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

purposes. The OPNAV 5511/12, "Classified Material Destruction Report" or another form may be used for this purpose. If used, destruction reports for Secret and Confidential material may be executed by only one witness to the destruction, and will be retained for 2 years.

16007. Destruction of Unclassified Material

1. Destroy copies of controlled unclassified information (e.g., FOUO, Sensitive Unclassified, and technical documents assigned distribution statements B through X) per SECNAVINST5210.8D, Navy and Marine Corps Records Disposition Manual. Copies will be disposed of by shredding. It will not be simply thrown into the trash or recycle bin.

2. Unclassified information, including formerly classified material that has been declassified, FOUO, and unclassified messages, do not require the assurance of complete destruction. Strip shredders are acceptable for destroying this type of information (except for Unclassified Drug Enforcement Administration (DEA) Sensitive Information and Naval Nuclear Propulsion Information (NNPI) which must be destroyed using classified destruction methods).

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

COMMAND LETTERHEAD

5510
MAD
(Date)

From: Security Manager
To: Department Head

Subj: AUTHORIZATION FOR ESTABLISHMENT OF SECONDARY CONTROL POINT

Ref: (a) Your Request for Authorization dtd _____
(b) Physical Security Evaluation
(c) SECNAV M-5510.36
(d) MCO P5510.18
(e) Sta(O) P5510.30

1. Your request contained in reference (a) is approved, based on information contained in reference (b).
2. You are authorized to store moderate quantities of classified material up to and including (Secret/Confidential) in GSA approved security containers/secure room/vault located within room_____, building_____.
3. You will ensure that all personnel under your cognizance who have access to the classified materials are thoroughly familiar with the contents of references (c) through (e).
4. This authority will become invalid upon any physical changes made in the storage area, any significant changes in the classification level, quantity or scope of the classified material to be stored, or any upgrading of minimum physical security requirements.

SIGNATURE

Copy to:
MAD

Figure 16-1. Sample Secondary Control Point Authorization Letter

CHAPTER 17

INDUSTRIAL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
Basic Policy	17000	17-2
Background	17001	17-2
Security Oversight to Cleared DOD Contractor Operations	17002	17-2
Contracting Officer's Representative (COR)	17003	17-3
Visits by Cleared DOD Contractor Employees	17004	17-3
Transmission or Transportation	17005	17-3
Disclosure	17006	17-4

CHAPTER 17

17-1

INDUSTRIAL SECURITY PROGRAM

17000. Basic Policy

1. Per Chapter 11 of reference (b), Commanding Officers will establish an industrial security program if their commands engage in classified procurement or when cleared DOD contractors operate within areas under their direct control.
2. An industrial security program is established at MCAS Yuma. Guidance, consistent with reference (b), is provided in this chapter to ensure that classified information released to industry is safeguarded.

17001. Background

1. Executive Order 12829, National Industrial Security Program, established the NISP for safeguarding classified information released to industry. Reference (b) implements the requirements of the NISP within the DON. Provisions of reference (b) relevant to operations of cleared DOD contractor employees entrusted with classified information will be applied by contract or other legally binding instrument.
2. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPRM), and DoD 5220.22-M Supp 1, imposes the requirements, restrictions, and safeguards necessary to prevent unauthorized disclosure of classified information released by U.S. Government executive branch departments and agencies to their contractors.
3. The Defense Industrial Security Clearance Office (DISCO), Columbus, OH, grants personnel clearances to individuals in private industry who require access to classified information in order to perform their jobs. The DISCO also grants Facility Security Clearances (FCLs) within the NISP.

17002. Security Oversight of Cleared DOD Contractor Operations.
There are two types of DOD Contractor operations onboard MCAS Yuma:

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

1. Tenant Activities. The DISCO will assume security oversight over classified work carried out by cleared DOD contractor employees at those activities which have been granted an FCL by the DISCO, and which have the status of a tenant activity.

17-2 Visitors. The Commanding Officer will maintain security oversight over classified work carried out by cleared DOD contractor employees in spaces controlled or occupied at this Station which do not warrant a FCL. These employees are considered to be long-term visitors. In this case, a classified visit request will be submitted to the MAD and the department where the work will be performed, per Chapter 11 of this Manual. Contractor employees will conform to command security regulations and will be included in the command security education program (see Chapter 4 of this Order). The Command Security Manager/Assistant Security Manager are delegated the security oversight responsibilities of all classified contracts aboard this installation.

17003. Contracting Officer's Representative (COR)

1. Per reference (b), a qualified security specialist will be designated, in writing, as a COR for the purpose of signing the Contract Security Classification Specification (DD 254), and revisions thereto. A DD 254 is required to be incorporated into each classified contract, and is designed to provide a contractor with the security requirements and classification guidance needed for performance on a classified contract.

2. Responsibilities of the COR are listed in reference (b).

17004. Visits by Cleared DOD Contractor Employees. Cleared contractors planning to visit MCAS Yuma for classified contract work will have their facility security officer submit a visit request in advance, by JPAS, message or fax, per paragraph 11002 of this Order. Visit requests hand carried by cleared DOD contractors will not be accepted. Visit requests received by the department to be visited will be routed to the MAD for verification of the contractor employee's security clearance. The responsibility for determining the need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit.

17005. Transmission or Transportation. Appropriately cleared and designated DOD contractor employees may act as couriers, escorts, or hand carriers provided that;

INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

1. They have been briefed by their facility security officer on their responsibility to safeguard classified information.

2. They possess an identification card or badge, which contains their name, photograph, and the company name. 17-3

3. They retain classified information in their personal possession at all times. Arrangements will be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability.

4. The transmission or transportation meets all other requirements specified in Chapter 15 of this Order and reference (b).

17006. Disclosure. Refer to reference (b) for guidance on disclosing classified information to contractors, including privately owned or proprietary information, export controlled technical data, and intelligence information.

CHAPTER 18

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
Definitions	18000	18-2
Reporting Responsibilities	18001	18-2
Preliminary Inquiry (PI)	18002	18-2
Actions Taken Upon PI Conclusion	18003	18-3
Reporting Losses or Compromise of Special Types of Classified Information and Equipment	18004	18-4
JAGMAN Investigations	18005	18-4
Unlocked Security Containers	18006	18-5
Discrepancies Involving Improper Transmissions	18007	18-5

CHAPTER 18

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

18000. Definitions

1. A loss of classified information occurs when it cannot be physically located or accounted for.
2. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access or a need-to-know. The unauthorized disclosure may have occurred knowingly, willfully, or through negligence.

18001. Reporting Responsibilities

1. Individual. Any individual who becomes aware that classified information is lost or compromised will immediately report the incident to the Command Security Manager or Assistant Security Manager. If that individual believes the Security Manager or Assistant Security Manager may be involved in the incident, the Commanding Officer will be notified. If the Commanding Officer is involved, MCIWEST must be notified. If circumstances of discovery make such notification impractical, the individual will contact the local NCIS office.
2. Security Manager. When a loss or compromise of classified information occurs, the Command Security Manager or Assistant Security Manager will immediately notify NCISRA, MCAS Yuma, and inform the Commanding Officer of the need to initiate a Preliminary Inquiry (PI). The Security Manager shall be responsible for overseeing the PI. The NCIS may or may not investigate.

18002. Preliminary Inquiry (PI). A PI is the initial process to determine the facts surrounding a possible loss or compromise. At the conclusion of the PI, a narrative of the PI findings is provided in support of recommended additional investigative or command actions. A PI is convened by the command with custodial responsibility over the lost or compromised information.

1. PI Initiation. When a possible loss or compromise of classified information occurs, the Commanding Officer will appoint, in writing, a command official (other than the Security Manager, Assistant Security Manager, or anyone involved with the

incident) to conduct a PI.

2. PI Submission

a. The PI must be completed within 72 hours of the initial discovery of the incident, and submitted in message or letter format to the Command Security Manager or Assistant Security Manager. The Command Security Manager /Assistant Security Manager will ensure the PI is properly prepared per reference (b).

b. If circumstances exist that would delay the completion of the PI within 72 hours, a request to extend the deadline will be submitted, in writing, to the Commanding Officer, the CNO (N09N2), the originator of the information, the Original Classification Authority (OCA) and the local NCIS office explaining the reason(s) for the delay. The Command Security Manager/Assistant Security Manager will notify the required recipients of the PI of the delay. Normally, the only reason for a delay should be due to a pending NCIS investigation when there is a need to preserve evidence.

3. PI Contents. Every effort will be made to keep the PI unclassified and without any enclosures. The PI will be prepared per reference (b).

18003. Actions Taken Upon PI Conclusion

1. If the PI concludes that a loss or compromise of classified information did occur, may have occurred, or a significant command security weakness(es) or vulnerability(ies) is revealed, the following actions will be taken:

a. The Command Security Manager or Assistant Security Manager will send the PI message or letter to the addressees listed in reference (b).

b. A JAGMAN Investigation will be initiated, prepared and submitted per the guidelines set forth in Chapter 12 of reference (b).

c. The Security Manager or Assistant Security Manager will notify the NCISRA, MCAS Yuma.

d. Additionally, the command will take any necessary disciplinary and/or corrective actions to prevent further damage

and/or recurrence.

2. If the PI concludes that a loss or compromise of classified information did not occur or the possibility of compromise is remote, the PI will not be submitted and all addressees required by reference (b) will be notified with a brief statement supporting the determination. However, if a minor security weakness or vulnerability is revealed due to the failure of a person(s) to comply with established security practices and/or procedures, any necessary disciplinary and/or corrective actions will be taken to prevent recurrence.

18004. Reporting Losses or Compromise of Special Types of Classified Information and Equipment

1. See reference (b) for actions to take if the following special types of classified information or equipment is lost or compromised:

- a. Computer systems, terminals, or equipment.
- b. Foreign Government Information (FGI).
- c. Restricted Data (including CNWDI) or Formerly Restricted Data.
- d. COMSEC information or keying material.
- e. Involving NATO classified information.

2. In all cases, the Command Security Manager or Assistant Security Manager will be apprised of the circumstances surrounding the loss or compromise.

18005. JAGMAN Investigations. A JAGMAN investigation is an administrative proceeding conducted per JAGINST 5800.7D, Manual of the Judge Advocate General. A JAGMAN investigation is usually convened by the command having custodial responsibility over the information lost or compromised. The Command Security Manager or Assistant Security Manager will provide oversight and assistance on the completion of JAGMAN investigations involving loss or compromise of classified information. The individual appointed to conduct the JAGMAN investigation will consult reference (b) on proper format and procedures for the JAGMAN investigation, and will consult with the Staff Judge Advocate (SJA) if any disciplinary action is contemplated.

18006. Unlocked Security Containers

1. If a container, vault or secure room in which classified material is stored is found unlocked in the absence of assigned personnel, the individual who discovered the unlocked security container, vault or secure room (e.g., a watchstander, guard or OOD) will immediately contact the custodian of the security container (listed on the SF 700 posted on the interior of the container). The individual finding the unlocked security container will lock the container while waiting for the custodian to arrive. The custodian will immediately inventory the contents of the container, vault or secure room to determine if any classified information has been removed.

2. The Command Security Manager or Assistant Security Manager will be notified of the incident as soon as possible. A PI will be initiated per the procedures described in paragraph 18002 above, and corrective action will be taken to prevent future instances from occurring.

18007. Discrepancies Involving Improper Transmissions

1. If classified information is received that appears to have been subjected to compromise, the Command Security Manager or Assistant Security Manager will immediately notify the forwarding command. Classified information will be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent where the contents are exposed, or it has been transmitted over unprotected communications circuits (e.g., fax, telephone, data links).

2. If the information was not subjected to compromise, but was improperly prepared or transmitted, the Command's Security Manager will notify the forwarding command using OPNAV 5511/51 (Security Discrepancy Notice) per reference (b).