



UNITED STATES MARINE CORPS

MARINE CORPS AIR STATION MIRAMAR
P O BOX 452000 SAN DIEGO CA 92145-2000

StaO P5510.3

CMCC

17 NOV 2003

STATION ORDER P5510.3

From: Commanding General
To: Distribution List

Subj: MARINE CORPS AIR STATION (MCAS) MIRAMAR INFORMATION AND
PERSONNEL SECURITY PROGRAM (SHORT TITLE: MCAS MIRAMAR
IPSP)

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) MCO P5510.18A

Encl: (1) Locator Sheet

1. Situation. To establish policies, guidelines and procedures governing the Information and Personnel Security Program within this command.

2. Mission. The Command Security Program is designed to adequately ensure maximum uniformity and effectiveness in the application of IPSP policies and procedures aboard MCAS Miramar. The Command Security Manager and Assistant Security Manager under the Assistant Chief of Staff, G-1 are responsible for coordinating and maintaining an effective IPSP.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To provide guidance for the execution of the IPSP, ensuring Commander's, Department Heads, and supervisors are fully aware of the requirements set forth in the IPSP and this Manual.

(2) Concept of Operations. The procedures set forth in this Manual supplement the aforementioned references, and will be used in conjunction to govern this command's IPSP. Where conflict with directives of higher authority exists, those directives will take precedence.

StaO P5510.3
17 NOV 2003

(3) Action. Commanding Officers, Department Heads and supervisors will ensure strict compliance with the guidance outlined in this Manual.

b. Subordinate Element Missions. Comply with the intent and content of this Manual.

c. Coordinating Instructions. Recommendations for changes to this Manual are invited and will be submitted to the Command Security Manager via the chain of command.

4. Administration and Logistics

a. This Manual is issued under Distribution Statement A and is published electronically. It can be accessed online via the MCAS Miramar web page at www.miramar.usmc.mil.

b. For the purpose of inspections, electronic files will suffice and need not be printed.

5. Command and Signal

a. Signal. This Manual is effective the date signed.

b. Command. The Manual is applicable to the Marine Corps Reserve and civilian employees supporting the Marine Corps.



P. C. CHRISTIAN
Chief of Staff

DISTRIBUTION: A

StaO P5510.3
17 NOV 2003

LOCATOR SHEET

Subj: MCAS MIRAMAR INFORMATION AND PERSONNEL SECURITY PROGRAM
(SHORT TITLE: MCAS MIRAMAR IPSP)

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

MCAS MIRAMAR 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

MCAS MIRAMAR IPSP

CHAPTER 1

INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	1000	1-3
OBJECTIVES	1001	1-3
RESPONSIBILITY FOR COMPLIANCE	1002	1-4
SPECIAL ACCESS PROGRAMS	1003	1-4
POLICY GUIDANCE	1004	1-4

MCAS MIRAMAR IPSP

CHAPTER 1

INTRODUCTION

1000. BASIC POLICY. The MCAS Miramar 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 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 Miramar 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 security awareness through education and familiarize personnel with the requirements for safeguarding classified information.
4. Security is a means, not an end. Rules, which govern the security of classified information, do not guarantee protection, and they do not attempt to meet every conceivable situation. All personnel who work with classified information must preserve a balance and common sense approach toward the subject. The ideal to be sought is the indoctrination of all personnel to the point they automatically exercise proper discretion in the exercise of their duties. Security of classified information then becomes a natural element of every task and not an additional burden. Command interest and involvement must be a priority.

1002. RESPONSIBILITY FOR COMPLIANCE

1. Commanding Officers and Department Heads are responsible for compliance and implementation of the MCAS Miramar IPSP within their respective units.
2. Each individual, military or civilian, in the Navy or Marine Corps, is individually responsible for complying with all aspects of this program, and are 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. SPECIAL ACCESS PROGRAMS

1. Sensitive Compartmented Information (SCI). The SCI program for MCAS Miramar is administered by the Special Security Office (SSO), 3d Marine Aircraft Wing (3d MAW). All requests for SCI billets, access, and interviews will be directed to that office via the Command Security Manager/Assistant Security Manager.
2. Critical Nuclear Weapon Design Information (CNWDI). The CNWDI program is a special access program that requires approval by the Commander, Marine Corps Air Bases Western Area. All personnel requiring assignment to the CNWDI program must submit a request to the Command Assistant Security Manager.

1004. POLICY GUIDANCE. Requests for guidance/interpretation concerning the contents of this Manual should be addressed by calling the Station Classified Material Control Center (CMCC) at 577-8624. In addition, telephone inquiries may be made directly to the CNO (N09N2) Security Action Hotline at (202) 433-8856.

MCAS MIRAMAR IPSP

CHAPTER 2

COMMAND SECURITY MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
COMMAND SECURITY RESPONSIBILITY AND IMPLEMENTATION	2000	2-3
COMMAND SECURITY MANAGER	2001	2-4
ASSISTANT SECURITY MANAGER	2002	2-4
DUTIES OF THE SECURITY MANAGER/ASSISTANT SECURITY MANAGER	2003	2-5
TOP SECRET CONTROL OFFICER	2004	2-7
PERSONNEL SECURITY COORDINATOR (PSC) .	2005	2-7
SECONDARY CONTROL POINT (SCP) CUSTODIAN	2006	2-9
OTHER SECURITY APPOINTMENTS	2007	2-10
ALL HANDS	2008	2-11
SECURITY REVIEWS AND INSPECTIONS . . .	2009	2-11
PLANNING FOR EMERGENCIES	2010	2-12
INTERNAL SECURITY PROCEDURES	2011	2-12

FIGURE

2-1	SAMPLE SECURITY MANAGER/ASSISTANT SECURITY MANAGER APPOINTMENT LETTER . . .	2-13
2-2	SAMPLE TOP SECRET CONTROL OFFICER APPOINTMENT LETTER	2-14

MCAS MIRAMAR IPSP

	<u>PAGE</u>
2-3 SAMPLE PERSONNEL SECURITY COORDINATOR APPOINTMENT LETTER	2-15
2-4 SAMPLE SECONDARY CONTROL POINT CUSTODIAN/ ALTERNATE CUSTODIAN APPOINTMENT LETTER	2-16
2-5 SECURITY REVIEW CHECKLIST	2-17

MCAS MIRAMAR IPSP

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. COMMAND SECURITY RESPONSIBILITY AND IMPLEMENTATION

1. The Commanding General (CG) is ultimately responsible for the implementation and effective management of the Information and Personnel Security Program within MCAS Miramar. The CG will appoint, in writing, a Security Manager and certain security personnel 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 subordinate units 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 at MCAS Miramar.
 - 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 the Security Manager, Assistant Security Manager, and all other DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of classified information, include a critical security element on which to be evaluated.

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

3. A network of security professionals is established throughout the command to supervise and ensure effective security management, and to fulfill the CG's responsibilities (see paragraphs 2001 through 2007).

2001. COMMAND SECURITY MANAGER

1. The Assistant Chief of Staff (AC/S), G-1 will normally be designated in writing as the Command Security Manager (see Figure 2-1). However, this duty may be designated to another qualified individual and/or to another department at the discretion of the CG. The Security Manager is the principal advisor on information and personnel security in the command, and is responsible to the CG 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.

2002. ASSISTANT SECURITY MANAGER

1. The Security Specialist will be designated in writing as the Command Assistant Security Manager (see Figure 2-1). The Assistant Security Manager carries out the provisions of the Information and Personnel Security Program at MCAS Miramar, and is responsible to the Command Security Manager for ensuring the program is inclusive of all requirements.

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 Information and Personnel Security Program at MCAS Miramar, and will be identified to all members of the command on organization charts, telephone listings, rosters, etc.

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 CG in matters pertaining to the security of classified information held at the command.

b. Serve as the principal advisor and representative to the CG 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 Manual.

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.

j. Maintain liaison with the 3d MAW SSO concerning SCI policies and procedures.

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

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

m. Coordinate with the Command Information Systems Security Manager on matters of common concern.

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

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

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

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

r. Ensure that all personnel who have had access to classified information who are separating or retiring have completed a Security Termination Statement.

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

2004. TOP SECRET CONTROL OFFICER. The Assistant Security Manager will be designated in writing as the Top Secret Control Officer (TSCO) (see Figure 2-2). The duties of the TSCO are listed in paragraph 2-3 of reference (b). The TSCO must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI completed within the previous 5 years.

2005. PERSONNEL SECURITY COORDINATOR (PSC)

1. Each Department/Section Head under the cognizance of CG, MCAS Miramar will designate, in writing, a Personnel Security Coordinator (PSC) (see Figure 2-3). The PSC will serve as liaison between department/section personnel and the Command Security Manager/Assistant Security Manager on matters concerning IPSP requirements, including security investigations, clearances, accesses, security training, and the continuous evaluation program. The PSC should be an individual senior enough to exercise authority to manage the IPSP within the department/section. A copy of the designation letter will be forwarded to the Command Security Manager. This individual may also be the designated Secondary Control Point (SCP) Custodian if the department/section maintains classified material. The PSC must be a U.S. citizen and must have a security clearance and access at or above the highest level of classified information held by the department/section.

2. Duties of the PSC include:

a. Monitor the clearances/accesses required by department/section personnel, military and civilian, and inform the Command Assistant Security Manager of any new or changing requirements. Ensure that all department/section personnel who will handle classified information or will be assigned to sensitive duties have an updated security investigation.

b. Ensure security clearances/accesses for department/section personnel who require access to classified information are requested using MARFORPAC Form 5510/1 (see Figure 9-1), and submitted to the Command Assistant Security Manager. Each request will contain a description of the duties that require the clearance/access.

c. Monitor completion and submission of security investigation and periodic reinvestigation requests by department/section personnel. Ensure the investigation/reinvestigation request is completed in a timely manner (30 days after notification), and submitted to the Command Assistant Security Manager for further processing.

d. Ensure that all department/section personnel, both military and civilian, attend security training as scheduled by the Command Assistant Security Manager. This includes the orientation briefing for new personnel, the annual security refresher briefing, counterintelligence briefings, and other special briefings described in Chapter 4 of this Manual.

e. Conduct security awareness training for department/section personnel to ensure they are familiar with the specific security functions required by the department/section. This training will be tailored to the individual, review procedures for handling and storing classified information in the areas the individual will handle it, and review any special security precautions within the department/section.

f. Ensure supervisors of individuals who have been granted access to classified information conduct on-the-job training to ensure that subordinates know the security requirements which impact on the performance of their duties.

g. Debrief personnel who have had access to classified information prior to their transfer from the department/section. Coordinate debriefing requirements with the Assistant Security Manager.

h. Keep the Command Security Manager or Assistant Security Manager apprised of any significant information that may have a bearing on an individual's continuing eligibility for a security clearance. Items to be reported are described in Appendices F and G of reference (a).

2006. 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 or section head will designate, in writing, a SCP Custodian and an alternate (see Figure 2-4). 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 Command Assistant Security Manager.

2. Personnel appointed as SCP Custodians or alternate custodians will certify that they have completed a sight inventory of all classified material maintained in the SCP.

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

2007. OTHER SECURITY APPOINTMENTS

1. Communications Security Material System (CMS) Custodian. A CMS Custodian (and alternate(s)) assigned to the G-6 Department will be designated in writing to maintain the Command's CMS account. The CMS Custodian is the principle advisor to the CG on matters concerning the security and proper handling of Communications Security (COMSEC) material and required records and reports. Duties and responsibilities of the CMS Custodian are outlined in CMS 21A. A copy of the appointment letter will be forwarded to the Command Security Manager.

2. Operations Security (OPSEC) Officer. An OPSEC Officer will be designated in writing to implement and manage the command OPSEC program per the guidelines set forth in MCO 3432.1, The Marine Corps Operations Security (OPSEC) Program; FMFM 3-54, Operations Security; and other references. Operational experience is essential to having a viable OPSEC Program. Thus, MCO 3432.1 requires the OPSEC Officer and function to be assigned to Station Operations (G-3). Duties and responsibilities of the OPSEC Officer are outlined in MCO 3432.1 and FMFM 3-54. The OPSEC Officer will coordinate security support for OPSEC surveys, assessments, and measures with the Command Security Manager. A copy of the appointment letter will be forwarded to the Command Security Manager.

3. Information Systems Security Manager (ISSM). An ISSM will be designated in writing to serve as the point of contact for all command Information Systems Security (INFOSEC) matters and to implement the Command's INFOSEC program. Information Systems Security Officer(s) (ISSOs) and Network Security Officer(s) (NSOs) will also be designated in writing, if appropriate, to implement and maintain the Command's information system and network security requirements. This appointment will be assigned to a commissioned officer or civilian employee GS-11 or higher from the G-6 Department. The ISSM is an Automated Information System (AIS) I Sensitive Position (see Chapter 5 of this Manual), and requires a favorably adjudicated SSBI completed within the previous 5 years. A copy of the appointment letter will be forwarded to the Command Security Manager.

4. Physical Security Officer. The Provost Marshal will be designated in writing as the Station Physical Security Officer. The duties and responsibilities of the Station Physical Security Officer are set forth in MCO P5530.14, Marine Corps Physical Security Program Manual.

5. Contracting Officer's Representative (COR). A COR will be designated for each classified contract per paragraph 2-6 of 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 Chapter 11 of reference (b) and Chapter 17 of this Manual are accomplished when classified information is provided to industry for performance on a classified contract.

2008. 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.

2009. 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 Programs using the self-inspection guides found in Appendix D of reference (a) and Exhibit 2C of reference (b).

2. SCP Custodians will conduct annual security reviews to evaluate the overall security posture of their respective areas, using Figure 2-5 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 Command Assistant Security Manager will inspect SCPs on an annual basis to assess compliance with the requirements for handling classified material per reference (b) and this Manual.

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

b. 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, the applicable Department/Section Head and the Command Security Manager will be notified.

2010. PLANNING FOR EMERGENCIES

1. Per paragraph 2-13 of reference (a) and paragraph 2012 of reference (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 Command Assistant Security Manager will develop and maintain the emergency action plan (EAP) for MCAS Miramar. The EAP will be maintained within the CMCC and each SCP.

2. In addition, each SCP will develop an emergency action plan 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 CMCC and the respective SCP.

2011. INTERNAL SECURITY PROCEDURES

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

2. Internal security procedures should include, but are not limited to: accounting and control of classified 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" is not considered adequate for internal security procedures.

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

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

From: Commanding General, Marine Corps Air Station, Miramar
To: Grade, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS COMMAND SECURITY MANAGER/ASSISTANT
SECURITY MANAGER

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) StaO P5510.3

1. Per the references, you are appointed as the Security Manager/Assistant Security Manager for this Command. You will be governed in your duties by the references and other applicable directives. You are directed to thoroughly familiarize yourself with them.

2. You will indicate by endorsement below that you are ready to assume the duties as the Command Security Manager/Assistant Security Manager.

SIGNATURE

(Date)

From: Grade, Name, SSN/MOS, USMC
To: Commanding General

1. I have read and understand the references and hereby assume the duties as the Security Manager/Assistant Security Manager for this Command.

SIGNATURE

Copy to:
CMCC

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

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

From: Commanding General, Marine Corps Air Station, Miramar
To: Grade, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) StaO P5510.3

1. Per the references, you are appointed as the Top Secret Control Officer for this Command. You will be governed in your duties by the references and other applicable directives. You are directed to thoroughly familiarize yourself with them.
2. You will indicate by endorsement below that you are ready to assume the duties as the Top Secret Control Officer.

SIGNATURE

(Date)

From: Grade, Name, SSN/MOS, USMC
To: Commanding General

1. I have read and understand the references and hereby assume the duties as the Top Secret Control Officer for this Command.

SIGNATURE

Copy to:
Security Manager

Figure 2-2. --Sample Top Secret Control Officer Appointment Letter

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

From: (Head, Department/Staff Section/Activity)

To: Grade, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS PERSONNEL SECURITY COORDINATOR

Ref: (a) StaO P5510.3
(b) SECNAVINST 5510.30A
(c) SECNAVINST 5510.36

1. You are appointed as the Personnel Security Coordinator for (Department/Staff Section/Activity) per reference (a). You will familiarize yourself with the requirements of the Information and Personnel Security Programs set forth in the references.

2. You will ensure that your duties and responsibilities outlined in reference (a) are carried out to the best of your ability. You will coordinate program requirements with the Command Security Manager, and will provide (department/section/activity) personnel assistance in solving security related problems.

3. You will indicate by endorsement below that you are ready to assume the duties as the (Department/Staff Section/Activity) Personnel Security Coordinator.

SIGNATURE

(Date)

From: Grade, Name, SSN/MOS, USMC

To: (Head, Department/Staff Section/Activity)

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

SIGNATURE

Copy to:
Security Manager

Figure 2-3. --Sample Personnel Security Coordinator Appointment Letter

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

From: (Head, Department/Staff Section/Activity)
To: Grade, Name, SSN/MOS, USMC

Subj: APPOINTMENT AS SECONDARY CONTROL POINT CUSTODIAN/
ALTERNATE CUSTODIAN

Ref: (a) StaO P5510.3
(b) SECNAVINST 5510.36

1. You are appointed as the Secondary Control Point (SCP) Custodian/Alternate Custodian for the (Department/Staff Section/Activity) 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 accounted for, you will assume the duties as the (Department/Staff Section/Activity) Secondary Control Point Custodian/Alternate Custodian.

SIGNATURE

(Date)

From: Grade, Name, SSN/MOS, USMC
To: (Head, Department/Staff Section/Activity)

1. I have become familiar with the duties to which I have been assigned. All classified material maintained by this SCP has been sighted and is accounted for. I have assumed my duties as the (Department/Staff Section/Activity) Secondary Control Point (SCP) Custodian/Alternate Custodian.

SIGNATURE

Copy to:
CMCC

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

MCAS MIRAMAR IPSP

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 SECNAVINST 5510.36?
8. Is there a current SF 700 envelope on file in the Station CMCC 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 SECNAVINST 5510.36, SECNAVINST 5510.30A, 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. Has there been any security violations since the last security review?

Figure 2-5. --Security Review Checklist

MCAS MIRAMAR IPSP

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?
15. Does the SCP have security awareness tools/products available and posted within their sections?
16. Has an inventory been conducted and all classified information accounted for?
17. Are inspection reports on file?
18. Have all discrepancies identified during the last security inspection been corrected? If not, why not?
19. Is there a current physical security survey/evaluation on file for the SCP?
20. Is there an emergency action plan on file at the SCP in the event of a natural disaster or civil disturbance?
21. Has a copy of the emergency action plan been forwarded to the Station CMCC?
22. Does the SCP have adequate destruction equipment available to meet the requirements of emergency destruction?
23. Has specific equipment been designated for the reproduction and shredding of classified information, and are signs prominently displayed on or near the equipment to advise users?
24. Have warning notices been posted on equipment not authorized for the reproduction or shredding of classified information?
25. Are requests to reproduce Secret information approved by the Command Security Manager or Assistant Security Manager?
26. Have all couriers hand carrying classified information been issued a DD 2501, Courier Authorization Card?

Figure 2-5. --Security Review Checklist - Continued

MCAS MIRAMAR IPSP

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	3000	3-3
ACTIVITIES TO BE REPORTED	3001	3-3

MCAS MIRAMAR IPSP

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/section 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 Miramar. 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 Miramar so appropriate counterintelligence action can be taken. If personnel desire, they may notify NCIS directly at (858) 577-4355/4361, 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, International Terrorism or Deliberate Compromise. Command personnel becoming aware of possible acts of sabotage (malicious damage), espionage, international 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.

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, and the circumstances surrounding the suicide or the attempted suicide.

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.

MCAS MIRAMAR IPSP

CHAPTER 4

SECURITY EDUCATION PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	4000	4-3
RESPONSIBILITIES	4001	4-3
SECURITY BRIEFINGS	4002	4-4
ADDITIONAL SPECIALIZED TRAINING	4003	4-6
COMMAND DEBRIEFING	4004	4-6
SECURITY TERMINATION STATEMENTS	4005	4-7
CONTINUING SECURITY AWARENESS.	4006	4-7
RECORDS	4007	4-8

MCAS MIRAMAR IPSP

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. PSCs are responsible for ensuring that all department/section personnel, both military and civilian, attend security training as scheduled by the Assistant Security Manager, and for conducting security awareness training within their department/staff section.
4. Supervisors 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 Assistant Security Manager will conduct security indoctrination training for new civilian employees being employed by the Department of the Navy for the first time, and who will handle classified material.
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 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 Assistant Security Manager 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. The department/section PSC will assist supervisors in identifying appropriate security requirements. 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 procedures, 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 Security Manager, Assistant Security Manager, Information Systems Security Manager/Officer, and/or other professional security sources will give this training.

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 Field Office San Diego schedules this training at MCAS Miramar, and promulgates the schedule by naval message.

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

a. Foreign Travel Briefing

(1) 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.

(2) In addition, military members traveling on orders or on personal leave overseas and civilian employees traveling on orders overseas are required to receive an antiterrorism briefing within six months prior to departure. This training may be completed online at the following address: <http://at-awareness.org>, access code "Aware."

b. New Requirements Briefings. Personnel whose duties would be impacted by changes in security policies or procedures will be briefed as soon as possible.

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

d. Training for Derivative Classifiers. The Security Manager/Assistant Security Manager will train derivative classifiers on an as required basis.

e. Training for Classified Couriers. The Security Manager/Assistant Security Manager will train classified couriers per paragraph 9-11 of 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:

a. Security Manager and Assistant Security Manager. These individuals will complete the Naval Security Manager Course taught by the NCIS Mobile Training Team (MTT) at Naval Air Station, North Island.

b. 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 Assistant Security Manager 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 Security Office in building 8630.

2. The Department/Staff Section PSC 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 CMCC.

3. The Command Assistant Security Manager, or designated representative, will debrief personnel who no longer require access to classified information when any of the following occur:

a. Terminating active military service or civilian employment.

b. DoD civilian employees temporarily separating for a period of 60 days or more, including sabbaticals and leave without pay status.

- c. Inadvertent substantive access to classified information which the individual was not eligible to receive.
- d. Security clearance eligibility revocation.
- e. 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, except for transferring from this command to another, must read and execute a Security Termination Statement (OPNAV 5511/14) at the time of debriefing by the Command Assistant Security Manager or designated representative.
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, except in certain situations described in paragraph 4-12 of reference (a).
3. If an individual refuses to sign the Security Termination Statement, the Command Assistant Security Manager 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 Assistant Security Manager 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 (MSRB).

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 which should be used to boost security awareness. These materials are available from the Command Assistant Security Manager. 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.

MCAS MIRAMAR IPSP

CHAPTER 5

NATIONAL SECURITY POSITIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	5000	5-3
DESIGNATION OF SENSITIVE POSITIONS . .	5001	5-3
CRITERIA FOR DESIGNATING SENSITIVE POSITIONS	5002	5-4
SUITABILITY AND SECURITY DETERMINATIONS	5003	5-7

FIGURE

5-1	SAMPLE POSITION SENSITIVITY MEMORANDUM	5-8
-----	--	-----

MCAS MIRAMAR IPSP

CHAPTER 5

NATIONAL SECURITY POSITIONS

5000. BASIC POLICY

1. National Security Positions are those that: 1) are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and 2) require 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, a material adverse effect on the national security. There are three sensitivity levels that apply to national security positions:

- a. Special-Sensitive (SS).*
- b. Critical-Sensitive (CS).
- c. Noncritical-Sensitive (NCS).

* Special Security Officer (SSO) Cognizance

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. The Security Manager is designated the command Position Sensitivity Officer and arbiter. Department Heads, in coordination with the Security Manager, will designate a position sensitivity level for each national security position (henceforth referred to as "sensitive" positions) under their control.

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 that is at a level higher than Critical 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.

(4) Category I AIS (High Risk) positions. Per DoD Directive 5200.2R, "Personnel Security Program," incumbents of Category I AIS positions have the following responsibilities:

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

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

(c) 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.

(d) 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 higher authority in the AIS-I category to insure the integrity of the system.

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

(f) Any other position designated by the Secretary of the Navy and/or his designee that involves relatively high risk for effecting grave damage or realizing significant personal gain.

(5) Any other position involving duties listed in paragraph 5-3 of reference (a), or so designated by the Secretary of the Navy and/or his designee.

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).

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

(4) Category II AIS (Moderate Risk) positions. Per DoD Directive 5200.2R, "Personnel Security Program," incumbents of Category II AIS positions have the responsibility for systems design, operations, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the AIS I category, including, but not limited to:

(a) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and government-developed privileged information involving award of contracts.

(b) Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.

(c) Any other position designated by the Secretary of the Navy and/or his designee that involves a degree of access to a system that creates a significant potential for damage or personal gain less than that in an AIS I position.

(5) Any other position involving duties listed in paragraph 5-3 of reference (a), or so designated by the Secretary of the Navy and/or his designee.

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. Satisfactory completion of a National Agency Check with Inquiries (NACI) is required for non-sensitive positions.

3. The CG has overall responsibility for ensuring that only those positions that meet the above criteria are designated as sensitive; and that the number of designated sensitive positions is held to the minimum consistent with mission requirements.

4. The process of designating sensitive positions is assigned to the Department Head of the position involved, in coordination with the Human Resources Office (HRO) Director, the ISSM for AIS risk determinations, and the Security Manager who is the arbiter. The position sensitivity will be determined for every DOD civilian position in the command and recorded in the memorandum format shown in Figure 5-1. The designation will be signed by the Command Security Manager.

5. The Assistant Security Manager will maintain a record of all position designation decisions, which will identify for each position: sensitivity level, required security or suitability investigation, level of access to classified information (or no access) and AIS level.

5003. SUITABILITY AND SECURITY DETERMINATIONS

1. Non-Sensitive Positions. Investigations for non-sensitive positions (NACI) require only a suitability determination. Command responsibility for employment suitability adjudications 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 (Access NACI (ANACI) or SSBI) 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. All other investigations, with actionable issues, will be forwarded by the DON CAF to the Command Security Manager for suitability adjudication before a security determination can be made. The Command Security Manager will follow the procedures in paragraph 5-5 of reference (a).

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

MEMORANDUM FOR THE RECORD

Subj: DESIGNATION OF POSITION SENSITIVITY, SECURITY CLEARANCE
AND PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

Ref: (a) SECNAVINST 5510.30A
(b) StaO P5510.3

1. Per the references, position sensitivity, security clearance level, and personnel security investigative requirements are certified, as indicated, for the following position:

- a. Position Description Number: PK008
- b. Position Title: COMPUTER SPECIALIST
- c. Grade/Series: GS-0324-11
- d. Position Sensitivity: Non-critical sensitive
- e. Security Clearance Level: Secret
- f. Required Investigation: ANACI
- g. AIS Risk: AIS Category II, Moderate Risk

2. Position sensitivity is based on the criteria found in reference (a), paragraph 5-3. The criteria most responsible for the sensitivity determination assigned is:

- a. Access to classified information
- b. AIS risk
- c. Other (specify)

Signature

Figure 5-1. --Sample Position Sensitivity Memorandum

MCAS MIRAMAR IPSP

CHAPTER 6

PERSONNEL SECURITY INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	6000	6-3
TYPES OF PERSONNEL SECURITY INVESTIGATIONS	6001	6-3
INVESTIGATIVE REQUIREMENTS	6002	6-3
PRE-SUBMISSION REQUIREMENTS	6003	6-5
PREPARATION AND SUBMISSION OF INVESTIGATIVE REQUESTS	6004	6-6
FOLLOW-UP ACTIONS ON INVESTIGATIVE REQUESTS	6005	6-7

MCAS MIRAMAR IPSP

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 CG, 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 Defense Security Service (DSS) and Office of Personnel Management (OPM) for the DON are described in Chapter 6 of reference (a).

6002. INVESTIGATIVE REQUIREMENTS

1. For 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 (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 5 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 (NACLIC) or Access National Agency Check with Written Inquiries (ANACI). Clearances granted based on investigations completed prior to NACLIC and ANACI implementation (1 March 1999) remain valid.

(a) For Secret clearances, the investigation must be updated every 10 years by a Secret Periodic Reinvestigation (SPR). As an exception, SPRs are required every 5 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 Confidential Periodic Reinvestigation (CPR).

c. All military and civilian investigation requests, except as noted in paragraph 2 below, will be submitted to the Command Assistant Security Manager for screening, completion, and forwarding to either DSS or OPM. PSCs will monitor and assist in this process to ensure follow-up and assistance as needed.

2. For Civilian Employment in Sensitive Positions

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

- (1) Nonsensitive position - NACI (SF-85).
- (2) Noncritical-Sensitive position - ANACI (SF-86).
- (3) Critical-Sensitive position - SSBI (SF-86).
- (4) Special-Sensitive position - SSBI (SF-86).

b. The Human Resources Office, MCAS Miramar is responsible for submitting investigation requests to determine suitability for federal employment of civil service employees appointed to sensitive and non-sensitive positions at MCAS Miramar. They will submit the appropriate investigation request (NACI, ANACI or SSBI) on employees new to federal employment or who have had more than a 24-month break in employment, per the requirements specified in paragraph 6-6 of reference (a). The HRO will coordinate requirements for security clearances with the Command Assistant Security Manager, as required.

3. For Specific Performance of Duty and Special Programs. The investigative requirements for personnel performing specific duties (e.g., Security Manager, cryptographic duties, AIS duties) and those mandated for certain programs (e.g., SCI, NATO) are described in paragraphs 6-8 and 6-9 of reference (a). These requirements will be coordinated with the Command Security Manager/Assistant Security Manager as necessary.

6003. PRE-SUBMISSION REQUIREMENTS. Before submitting a PSI request to the DSS or OPM, the Command Assistant Security Manager 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) and/or the Defense Clearance and Investigations Index (DCII). (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). A 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. The LRC will be recorded on MARFORPAC Form 5510/1 (see Figure 9-1) and retained in security files until transfer, termination, or retirement of the individual. Procedures for completing the MARFORPAC Form 5510/1 are set forth in Chapter 9 of this Manual.
3. Validate Citizenship. The Assistant Security Manager will verify that the individual is a United States citizen, using the guidelines contained in Appendix I of reference (a).
4. Verify Date and Place of Birth and Education. When requesting an SSBI, the Assistant Security Manager 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 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 either the Electronic Personnel Security Questionnaire (EPSQ) software program or Standard Form (SF) 86, Questionnaire for National Security Positions.
2. Investigative requests will be completed per guidance provided by the Command Assistant Security Manager. PSCs will make themselves available to assist individuals with completing the forms as needed. Upon completion and validation of the EPSQ or SF86, the individual will transmit their form to the Assistant Security Manager for further processing (or to the HRO, MCAS Miramar if the request is for a new federal civilian employee, per paragraph 6002 above).
3. The Command Assistant Security Manager will review and validate the investigation request forms for completeness, accuracy, and identification of any security problems; and will transmit the completed, validated, and signed PSI requests to the appropriate investigative agency (DSS or OPM).

4. The Assistant Security Manager will maintain a copy of the PSI request in the individual's local security file for future tracer actions and to aid personnel with future reinvestigation questionnaire requirements. If the PSI request is submitted electronically via the EPSQ to DSS, a copy of the EPSQ receipt (posted at www.dss.mil) will also be maintained.

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 effect 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. The Assistant Security Manager will conduct follow-up actions with DSS and OPM as needed until the investigation is complete and DON CAF makes the clearance determination, per paragraph 6-16 of 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 Assistant Security Manager will notify DSS or OPM accordingly.

2. The guidance regarding Marine Corps tracer action through the MCTFS is invalid. Tracer actions for Marines must be submitted to the DON CAF.

3. In the event a military member receives orders to transfer while an investigation is pending, the Assistant Security Manager will ensure the paper copy of the PSI request is forwarded to the gaining command's security office.

MCAS MIRAMAR IPSP

CHAPTER 7

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	7000	7-3
PERSONNEL SECURITY PROGRAM RESPONSIBILITIES	7001	7-3
PERSONNEL SECURITY DETERMINATIONS . .	7002	7-4
UNFAVORABLE DETERMINATIONS PROCESS . .	7003	7-5
APPEALING UNFAVORABLE DETERMINATIONS .	7004	7-5

MCAS MIRAMAR 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 Manual 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 primary and special staff sections. They are responsible for reviewing information available locally 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 ensure the command responsibilities listed in paragraph 7-2g of 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 Appendix G of 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 Chapter 10 of reference (a) and Chapter 10 of this Manual); 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 CG (for civilian personnel) or the Commanding Officer, Headquarters and Headquarters Squadron (HQHQRON) (for military personnel), at 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-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, division officer, supervisors, 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 equity to the subject and the protection of national security.

7003. UNFAVORABLE DETERMINATIONS 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 paragraph 7-7 of reference (a) when a LOI is received by this command.

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 paragraph 7-8 of reference (a).

MCAS MIRAMAR IPSP

CHAPTER 8

CLEARANCES

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	8000	8-3
CITIZENSHIP	8001	8-3
INTERIM SECURITY CLEARANCES	8002	8-4
DENIAL OR REVOCATION OF SECURITY CLEARANCE	8003	8-5
REESTABLISHING A SECURITY CLEARANCE AFTER A DENIAL OR REVOCATION	8004	8-5

MCAS MIRAMAR 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 Defense Clearance and Investigations Index (DCII) or a DON CAF certification message may also be used in lieu of the JPAS. 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. Paragraphs 5-7 and 9-16 of reference (a) describe 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 Chapter 12 of reference (b).

3. The Assistant Security Manager 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 Appendix I of reference (a). U.S. citizens who hold a current, valid security clearance issued by the DON CAF do not have to submit evidence of citizenship to retain clearance at or below the same level.

8002. INTERIM SECURITY CLEARANCES

1. Interim clearances are granted temporarily at the command level pending completion of full investigative requirements and pending establishment of security clearance eligibility by the DON CAF.

2. Interim clearances may be granted for up to one year, 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.

d. There is no information included on the PSI request or discovered during the LRC which would reflect unfavorably on the individual's loyalty, reliability, or trustworthiness.

3. The Command Security Manager and Assistant Security Manager are delegated the authority to grant interim clearances and the associated access under the conditions specified in paragraph 8-5 of reference (a).

4. Interim clearances may, if necessary, be extended beyond one year provided an extension request is submitted to the DON CAF. If DON CAF denies an extension request, the individual's interim clearance will be withdrawn and the associated access will be suspended.

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 paragraph 9-18 of 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 Manual, that suggests an individual may no longer be in compliance with personnel security standards, the Command Security Manager or Assistant Security Manager will report the issues to the DON CAF for adjudication. Exhibit 10A of reference (a) provides a checklist of issues that must be reported.

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 paragraph 7-7 of 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 Command Assistant Security Manager will remove all accesses authorized, and debrief the individual per paragraph 4-11 of reference (a), including execution of a Security Termination Statement.

8004. REESTABLISHING A SECURITY CLEARANCE AFTER A DENIAL OR REVOCATION. 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 Appendix G of reference (a), and will include a letter of recommendation from the individual's department head. Interim security clearances and/or access and assignment to sensitive civilian positions are not authorized until the DON CAF reestablishes the security clearance.

MCAS MIRAMAR IPSP

CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	9000	9-3
REQUESTING ACCESS	9001	9-3
LOCAL RECORDS CHECK	9002	9-4
GRANTING ACCESS TO CLASSIFIED INFORMATION	9003	9-4
CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312)	9004	9-5
PERSONAL ATTESTATION	9005	9-6
RECORDING COMMAND ACCESS	9006	9-6
TEMPORARY ACCESS UNDER INTERIM CLEARANCE PROCEDURES	9007	9-8
PERIODIC REINVESTIGATION REQUIREMENTS	9008	9-8
OTHER SPECIAL ACCESSES	9009	9-9
ACCESS BY INVESTIGATIVE AND LAW ENFORCEMENT AGENTS	9010	9-10
TERMINATING, WITHDRAWING OR ADJUSTING ACCESS	9011	9-10
SUSPENSION OF ACCESS FOR CAUSE	9012	9-11
ACCESS TO CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)	9013	9-12

MCAS MIRAMAR IPSP

	FIGURE	<u>PAGE</u>
9-1	SAMPLE MARFORPAC FORM 5510/1, "REQUEST FOR ACCESS TO CLASSIFIED MILITARY INFORMATION (CMI) & LOCAL RECORDS CHECK"	9-13

MCAS MIRAMAR IPSP

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, division and branch heads will request access for civilian and military personnel under their jurisdiction by completing Section I of MARFORPAC Form 5510/1 (see Figure 9-1) and forwarding it to the Command Assistant Security Manager. Requests for access will be provided on an individual basis (i.e., one person per request). Requests for access will also be accomplished as part of the checking-in procedures when incoming personnel check in with the Security Office.

9002. LOCAL RECORDS CHECK (LRC). The Command Assistant Security Manager will forward MARFORPAC Form 5510/1 to Medical, the Provost Marshall's Office (PMO), and the applicable personnel office (HRO for civilian employees or HQHQRON for military personnel) for the 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. Medical, PMO, and the applicable personnel office will ensure they complete Sections II, III and IV of MARFORPAC Form 5510/1, respectively, and return the form to the Assistant Security Manager without delay. A summary of any unfavorable information found or copies of relevant documents will be attached in a sealed envelope and returned with the form.

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 Chapter 9 of 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 an interim clearance or continuing access (see paragraphs 9007 and 9008 herein).

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

c. The LRC indicates no disqualifying information (if it does, the procedures in paragraph 7002 of this Manual 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. Interim clearance procedures are not employed in this situation.

9004. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312)

1. Per paragraph 9-4 of 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 Command Assistant Security Manager will report the refusal to the DON CAF.

2. The Assistant Security Manager will ensure all military and civilian employees who have not previously executed a SF 312 (or one of its predecessors) sign a current SF 312 before being given access. Prior execution of a SF 312 may be indicated by:

a. For Marine Corps personnel - Documenting the execution of a SF 312 is effected via the unit diary and in the JPAS. Before 23 August 1999, an entry was made on the SRB/OQR Page 11. Therefore, in addition to screening SRB/OQR entries, the MCTFS and JPAS will be queried to ascertain if a Marine has previously executed a SF 312.

b. For DON civilian personnel - the previously executed SF 312 may be in the Official Personnel Folder (OPF).

3. The Command Security Manager and Assistant Security Manager are authorized to accept the SF 312 on behalf of the U.S. Government.

4. The Assistant Security Manager will forward executed SF 312's as follows:

a. For Marine Corps personnel - Headquarters U.S. Marine Corps (MMSB-22).

b. For Navy personnel - Bureau of Naval Personnel (Pers 313C1).

c. For DON civilian employees - HRO, MCAS Miramar 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. This attestation is not a legally binding oath and will not be sworn to.

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

9006. RECORDING COMMAND ACCESS

1. Personnel Security Database. Per paragraph 9-5 of reference (a), the Command Assistant Security Manager will maintain a computerized Personnel Security database of all clearances and accesses granted to command civilian and military personnel, to include temporary accesses, special accesses, and other program accesses formally granted (e.g., CNWDI).

2. Command Security Access List (CSAL)

a. The Assistant Security Manager will periodically provide a CSAL generated from the database to all departments and staff sections. Upon request, special access listings will also be generated for only those personnel assigned to a specific department, branch, or staff section. PSCs and/or department heads will review this listing and will submit any requested changes and/or questions to the Command Assistant Security Manager.

b. Departments and staff sections will maintain the CSAL to provide verification of individuals requiring access to classified information. Custodians of classified information will use this listing to provide verification of authorized access before allowing others access to classified information.

3. Joint Personnel Adjudication System (JPAS). The Command Assistant Security Manager 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).

4. Access Letters. The Command Assistant Security Manager will forward an access letter to the individual when access has been granted. This letter will serve as verification of access when requesting receipt and draw authority if a current copy of the CSAL is not available.

5. Individual Security File. In addition, the Command Assistant Security Manager will maintain individual case files in support of the Personnel Security database and JPAS entries. The individual case file will be retained for two years following access termination per paragraph 9-5 of reference (a).

9007. TEMPORARY ACCESS UNDER INTERIM CLEARANCE PROCEDURES

1. If the DCII or 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 Top Secret access, the individual must have current Secret security clearance eligibility, or a favorable investigation completed within the last ten years, with no break in service exceeding 24 months. See paragraph 8002 of this Manual 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:

a. Access to Top Secret or SCI information - the investigation must have been completed within the previous 5 years.

b. Access to Secret information - the investigation must have been completed within the previous 10 years.

c. Access to Confidential information - the investigation must have been completed within the previous 15 years.

2. As an exception to this policy, any person who has less than one year before retirement, resignation, or separation may continue to be authorized access if required for operational exigencies.

3. The Command Assistant Security Manager will notify personnel 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 (without prejudice to the individual). 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. Paragraphs 9-6 through 9-16 of reference (a) contain procedures and restrictions for granting access to classified information in special circumstances.

2. 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, participate in advancement exams, 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.

g. Access for historical researchers.

h. Limited Access Authorization for non-U.S. citizens.

9010. 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.

9011. TERMINATING, WITHDRAWING OR ADJUSTING ACCESS. Paragraphs 8-9 and 9-17 of reference (a) outline the requirements for terminating, withdrawing, and adjusting clearances and access.

1. Access terminates when an individual transfers from a command. Personnel who are transferring from this command to another will be debriefed per paragraph 4-11 of reference (a) and paragraph 4004 of this Manual. A Security Termination Statement is not required.

2. The Command Assistant Security Manager 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 Assistant Security Manager will debrief the individual per paragraph 4-11 of reference (a) and paragraph 4004 of this Manual. Execution of a Security Termination Statement is required.

3. The Assistant Security Manager 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.

4. The Assistant Security Manager 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.

5. Department Heads or PSCs will submit requests for the termination of access by Station personnel in writing (may be e-mail) to the Command Assistant Security Manager upon the occurrence of one of the following:

a. Reported derogatory information to include alcohol or drug abuse.

b. When access is no longer required in the performance of military duties.

6. 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 paragraph 9-18 of reference (a).

9012. SUSPENSION OF ACCESS FOR CAUSE

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the CO HQHQRON (for military personnel) or the CG (for civilian personnel) may suspend access, at the recommendation of the Command Security Manager/Assistant Security Manager, per the procedures discussed in paragraph 7002 of this Manual. 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 paragraph 9-18 of reference (a) will be followed.

9013. 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 Command Assistant Security Manager is responsible for processing requests for CNWDI access, and will execute the following procedures, as set forth in paragraph 9-19 of reference (a):

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

b. Ensure only U.S. citizens are authorized access to CNWDI.

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

d. Brief personnel requiring access to CNWDI on its sensitivity. Record the access authorization in the MCAS Miramar Personnel Security database and in JPAS, and maintain briefings and access authorizations in appropriate security records.

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

f. Prepare/maintain appropriate records and reports.

MCAS MIRAMAR IPSP

REQUEST FOR ACCESS TO CLASSIFIED MILITARY INFORMATION (CMI) & LOCAL RECORDS CHECK			
<p>PRIVACY ACT STATEMENT: Personal information solicited by this form required for facilitating access to CMI. Failure to provide requested information could result in denial of access. Personal information solicited is subject to safeguarding under the Privacy Act of 1974, per USC 5, 301 Departmental Regulations.</p>			
SECTION I (REQUEST) (APPLICABLE FOR MILITARY AND CIVILIAN EMPLOYEES)			
TO Command Security Manager, Marine Corps Air Station Miramar/Marine Corps Air Bases Western Area Miramar		FROM (DEPARTMENT/SPECIAL STAFF SECTION)	
NAME (LAST, FIRST, MIDDLE)		RANK(MIL) GRADE (CIV)	SSN
DATE OF BIRTH	PLACE OF BIRTH (CITY/STATE)	COUNTRY OF BIRTH (IF NOT USA)	DATE
MILITARY BILLET DESCRIPTION, CIVILIAN POSITION DESCRIPTION OR CIVILIAN CONTRACTOR JOB TITLE			
CHECK ONE	ACTIVE DUTY <input type="checkbox"/>	RESERVE <input type="checkbox"/>	CIV SVC <input type="checkbox"/>
POSITION SENSITIVITY (CHECK ONE) (Applicable to Military, Civ Employees, and Contractors)		Non-Critical Sensitive (NCS) <input type="checkbox"/>	Critical Sensitive (CS) <input type="checkbox"/>
PRINTED NAME/RANK OF DIVISION/SPECIAL STAFF SECTION OFFICIAL		SIGNATURE OF DIVISION/SPECIAL STAFF SECTION OFFICIAL	
SECTION II (MEDICAL) (APPLICABLE FOR MILITARY PERSONNEL ONLY)			
DO THE MEDICAL RECORDS OF THIS INDIVIDUAL REVEAL ANY UNFAVORABLE INFORMATION CONCERNING A PAST/PRESENT HISTORY OF MENTAL OR NERVOUS DISORDERS, DRUG OR ALCOHOL ABUSE, SEXUAL PERVERSION OR EVIDENCE OF ACTS OR BEHAVIORAL TRAITS INDICATING A LACK OF JUDGEMENT, STABILITY, RELIABILITY OR TRUSTWORTHINESS?			
(CHECK ONE)			
<input type="checkbox"/> RECORDS AVAILABLE, NO UNFAVORABLE INFORMATION INDICATED.			
<input type="checkbox"/> NO RECORDS AVAILABLE			
<input type="checkbox"/> RECORDS AVAILABLE, UNFAVORABLE INFORMATION WAS FOUND. A SUMMARY OF THE UNFAVORABLE INFORMATION OR COPIES OF RELEVANT DOCUMENTS ARE ATTACHED IN A SEALED ENVELOPE.			
DATE	PRINTED NAME/RANK OF MEDICAL OFFICIAL CONDUCTING RECORDS CHECK		SIGNATURE
SECTION III (PROVOST MARSHAL) (APPLICABLE FOR MILITARY AND CIVILIAN EMPLOYEES)			
(CHECK ONE)			
<input type="checkbox"/> RECORDS AVAILABLE, NO UNFAVORABLE INFORMATION INDICATED.			
<input type="checkbox"/> NO RECORDS AVAILABLE			
<input type="checkbox"/> RECORDS AVAILABLE, UNFAVORABLE INFORMATION WAS FOUND. A SUMMARY OF THE UNFAVORABLE INFORMATION OR COPIES OF RELEVANT DOCUMENTS ARE ATTACHED IN A SEALED ENVELOPE.			
DATE	PRINTED NAME/RANK OF PMO OFFICIAL CONDUCTING RECORDS CHECK		SIGNATURE
SECTION IV (PERSONNEL) (APPLICABLE FOR MILITARY AND CIVILIAN EMPLOYEES, LESS CONTRACTORS)			
NO BREAK IN FEDERAL SERVICE SINCE INSERT DATE: _____ (APPLICABLE FOR MILITARY PERSONNEL AND CIVILIAN EMPLOYEES)			
(FEDERAL SERVICE INCLUDING ALL ACTIVE DUTY AND RESERVE COMPONENTS OF THE MILITARY, NATIONAL GUARD, ROTC, MILITARY ACADEMIES, AND EMPLOYMENT WITH OTHER FEDERAL AGENCIES)			
DCTB (N/A FOR CIVILIAN EMPLOYEES)	EAD (N/A FOR CIVILIAN EMPLOYEES)		AFADBD (N/A FOR CIVILIAN EMPLOYEES)
<input type="checkbox"/> YES <input type="checkbox"/> NO	U.S. CITIZENSHIP VERIFICATION (APPLICABLE FOR MILITARY/CIVILIAN EMPLOYEES)		
<input type="checkbox"/> YES <input type="checkbox"/> NO	DOES THE SRB/OQR/OPF CONTAIN UNFAVORABLE INFORMATION ON INDIVIDUAL'S INTEGRITY, DISCRETION, TRUSTWORTHINESS, OR LOYALTY TO THE U.S.? (IF YES, A COPY OF UNFAVORABLE RECORDS ATTACHED IN A SEALED ENVELOPE) (APPLICABLE FOR MILITARY/CIVILIAN EMPLOYEES)		
<input type="checkbox"/> YES <input type="checkbox"/> NO	IS THE INDIVIDUAL UNDER INVESTIGATION, CHARGED, AWAITING TRIAL, TRIED AND CONVICTED, OR IS A CASE PENDING BEFORE A COURT OR BOARD OF INQUIRY? (N/A FOR CIVILIAN EMPLOYEES)		
<input type="checkbox"/> YES <input type="checkbox"/> NO	DOES THE SRB/OQR/OPF REFLECT THAT THE INDIVIDUAL HAS A SIGNED CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT, SF 312, SF 189 OR SF 189A? (APPLICABLE FOR MILITARY/CIVILIAN EMPLOYEES) IF YES, DATE SIGNED: _____		
DATE	PRINTED NAME OF PERSONNEL OFFICIAL CONDUCTING RECORDS CHECK		SIGNATURE
REMARKS			

MARFORPAC FORM 5510/1
REV AUG01 (Modified for internal MCAS Miramar use only)

Figure 9-1. --Sample MARFORPAC FORM 5510/1, "Request For Access To Classified Military Information (CMI) & Local Records Check"

MCAS MIRAMAR IPSP

CHAPTER 10

CONTINUOUS EVALUATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	10000	10-3
REPORTING REQUIREMENTS	10001	10-3
PROGRAM ELEMENTS	10002	10-4
COMMAND REPORTS OF LOCALLY DEVELOPED UNFAVORABLE INFORMATION	10003	10-5

MCAS MIRAMAR IPSP

CHAPTER 10

CONTINUOUS EVALUATION

10000. BASIC POLICY. Reference (a) requires that each individual with access to classified information be evaluated continuously to ensure that they remain eligible for a security clearance. The continuous evaluation program will rely on all personnel within this command to report questionable or unfavorable information that may be relevant to a security clearance determination.

10001. REPORTING REQUIREMENTS

1. In support of this program:

a. Individuals will be encouraged to report to their supervisor, their PSC, their Department, Section or Branch Head, or the Command Security Manager/Assistant Security Manager, and seek assistance for any incident or situation affecting their continued eligibility for access to classified information. To accomplish this objective, personnel will be briefed on pertinent security regulations and standards of conduct required of all individuals holding positions of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility to assess classified information rests with the individual.

b. All command elements and/or Department Heads, particularly HRO, HQHQRON, PMO, Legal, Medical officials, and supervisory personnel, will advise the Command Security Manager/Assistant Security Manager when they become aware of information which could place in question an individual's loyalty, reliability, or trustworthiness. In addition, any relevant documents (e.g., military police reports, NCIS reports, copies of investigation reports, copies of Article 15 proceedings, medical reports, psychiatric evaluations, etc.) will be forwarded to the Command Security Manager/Assistant Security Manager. This information must be evaluated from a security perspective to determine its significance.

c. Co-workers have an obligation to advise their supervisor, their PSC, their Department, Section or Branch Head, or the Command Security Manager/Assistant Security Manager when they become aware of information with potential security clearance significance.

d. Supervisors and managers have a responsibility to detect an individual's problems at an early stage. They will direct 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 Manual. 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 paragraph 10-4 of reference (a), the Command Security Manager, Assistant Security Manager, 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 Command Assistant Security Manager will report that information to the DON CAF, per paragraph 8-10 and Exhibit 10A of reference (a). All information which meets the standards outlined in Appendix F of reference (a) will be reported, without attempting to apply or consider any mitigating factors that may exist.

2. If circumstances warrant, the individual's access to classified information will be suspended for cause. The suspension action will be accomplished per paragraph 9-18 of reference (a).

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

4. In cases where unfavorable information has been resolved by local investigation or inquiry, the Command Assistant Security Manager 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.

MCAS MIRAMAR IPSP

CHAPTER 11

VISITOR CONTROL

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	11000	11-3
CLASSIFIED VISIT REQUEST PROCEDURES .	11001	11-4
CLASSIFIED VISITS TO MCAS MIRAMAR . .	11002	11-4
VISITS BY FOREIGN NATIONALS AND REPRESENTTIVES OF FOREIGN ENTITIES . .	11003	11-6

MCAS MIRAMAR IPSP

CHAPTER 11

VISITOR CONTROL

11000. BASIC POLICY

1. For security purposes, the term visitor means:

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

b. Individuals assigned to temporary additional duty (TAD) to MCAS Miramar. Personnel on temporary duty orders, reservist 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 Miramar 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 restricted 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. Visitor policy for the general public is defined in StaO 5530.2, Physical Security Plan. 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. The general public will not be permitted access to restricted areas at any time.

11001. CLASSIFIED VISIT REQUEST PROCEDURES

1. MCAS personnel will inform the Assistant Security Manager 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 request:

- a. Activity to be visited.
- b. Dates and duration of the visit.
- c. Reason for the visit.
- d. Level of access required.
- e. A point of contact, if known.
- f. The fax number of the activity to be visited.

2. Visitors requiring access to classified information must ensure they have the appropriate clearance and any special access authorizations required for the visit. If necessary, a security investigation request will be initiated. This must be determined in sufficient time to complete and submit all required documentation before the individual departs this command.

3. The Assistant Security Manager will submit the visit request to the activity being visited per paragraph 11-2 of reference (a).

4. Under no circumstances will personnel handcarry their own visit request to the places being visited. Hand carried orders do not contain the required information and, therefore, cannot be used in lieu of visit requests.

11002. CLASSIFIED VISITS TO MCAS MIRAMAR

1. A visit request will be required in writing for any individual visiting MCAS Miramar departments and staff sections who requires access to classified information. Visit requests received from other commands and activities will be routed to the Command Assistant Security Manager for information and coordination

purposes. The Assistant Security Manager will verify security clearances through accessing the DCII or JPAS, send a copy of the visit request to the department or staff section to be visited, and coordinate any special requirements 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 be requested to call their parent command/company to ask them to pass their security clearance to the Command Security Manager. Individuals are not permitted to handcarry their own security clearance to MCAS Miramar.

4. All departments and divisions 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 Accounting Office (GAO) are described in Chapter 11 of reference (a).

11003. VISITS BY FOREIGN NATIONALS AND REPRESENTATIVES OF FOREIGN ENTITIES

1. SECNAVINST 5510.34, Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations, and paragraph 11-3 of reference (a) provide guidance on visits by foreign nationals and representatives of foreign entities.

2. All foreign visitors to MCAS Miramar must have a Foreign Visit Request (FVR) submitted by their country's Embassy that has been processed by the Foreign Disclosure Control Division of the Navy International Programs Office. FVRs received at MCAS Miramar will be immediately forwarded to the Command Assistant Security Manager.

3. The Assistant Security Manager will:

a. Liaise with the Protocol Officer, or the Department/Staff Section with cognizance for the foreign visit.

b. Reply with concurrence or nonconcurrence to the Foreign Disclosure Office.

c. Provide copies of the FVR to the PMO.

d. Maintain files on all FVRs for two years after the last day of the visit.

MCAS MIRAMAR IPSP

CHAPTER 12

CLASSIFICATION MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	12000	12-3
CLASSIFICATION LEVELS	12001	12-3
CLASSIFICATION DETERMINATION	12002	12-3
ACCOUNTABILITY OF CLASSIFIERS	12003	12-4
CLASSIFICATION GUIDANCE	12004	12-4
SECURITY CLASSIFICATION GUIDES	12005	12-5

MCAS MIRAMAR IPSP

CHAPTER 12

CLASSIFICATION MANAGEMENT

12000. BASIC POLICY. Executive Order 12958 is the only basis for classifying NSI, 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 the 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," "Sensitive Unclassified," or "Secret Sensitive" are not security classifications and will not be used to identify U.S. classified information.

12002. CLASSIFICATION DETERMINATION. Classified material when drafted receives either an original classification or derivative classification determination.

1. Original Classification. Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure. This decision can be made only by Original Classification Authorities (OCAs), who have been specifically granted the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information. No official at MCAS Miramar has original classification authority. Referrals regarding original classification will be made to Commander, Marine Forces, Pacific, who has original classification authority at the Top Secret level.

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).

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, intelligence control markings, declassification instructions, and a "Derived From" statement indicating the classified source(s).

12003. ACCOUNTABILITY OF CLASSIFIERS. Originators of classified documents are accountable for the accuracy of their classification decisions. Those with command signature authority must ensure that classification markings, if used, are correct. The Command Security Manager or Assistant Security Manager will review all command-originated classified documents to ensure correct classification and marking. The Command Security Manager is delegated the authority to approve all derivative classification decisions.

12004. CLASSIFICATION GUIDANCE. Inasmuch as it is impractical to cover all subjects dealing with classifying information, originators of classified documents will review Chapter 4 of reference (b) for guidance on the following:

1. Limitations on classifying.
2. Duration of original classification/exemption categories.
3. Classification challenges.
4. Tentative classification.
5. Foreign government information.
6. Authority to downgrade, declassify, or modify classified information.
7. Declassification reviews.

12005. SECURITY CLASSIFICATION GUIDES. Security Classification Guides (SCGs) are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements. They are prepared by OCAs for each DON system, plan, program, or project under their cognizance which creates classified information. Additional information concerning security classification guides is contained in Chapter 5 of reference (b).

MCAS MIRAMAR IPSP

CHAPTER 13

MARKING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	13000	13-3
REPRODUCTION OF GUIDES	13001	13-3
MARKING CLASSIFIED FILES, FOLDERS AND GROUPS OF DOCUMENTS	13002	13-4
MARKING REMOVABLE AUTOMATED INFORMATION SYSTEM (AIS) STORAGE MEDIA	13003	13-4
MARKING E-MAIL TRANSMITTED ON THE SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)	13004	13-5

MCAS MIRAMAR IPSP

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 paragraph 6-1.5 of 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.

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 the material is classified, to tell the user the degree of protection required, 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 Chapter 6 of reference (b). The Command Assistant Security Manager will provide assistance as needed.

13001. REPRODUCTION OF GUIDES. The reproduction of guides using Chapter 6 and exhibits 6A-1 through 6A-18 of reference (b) is encouraged for use by personnel responsible for proper marking of classified material.

13002. 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 Miramar are as follows:

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

13003. 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:

- Sensitive Unclassified - SF 710 (Green)
- Confidential - SF 708 (Blue)
- Secret - SF 707 (Red)
- 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, disk cartridges, disk packs, diskettes, and magnetic cards. See Exhibit 6A-18 of reference (b) for placement instructions.

13004. 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 the same as they would for 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 (usually just above the salutation).

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 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.

MCAS MIRAMAR IPSP

CHAPTER 14

SAFEGUARDING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	14000	14-3
RESPONSIBILITY	14001	14-3
CONTROL MEASURES	14002	14-4
CLASSIFIED MESSAGES	14003	14-5
SIPRNET E-MAIL AND OTHER ELECTRONICALLY TRANSMITTED MATERIAL	14004	14-5
WORKING PAPERS	14005	14-5
SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION .	14006	14-6
PROCESSING CLASSIFIED INFORMATION ON INFORMATION SYSTEMS	14007	14-7
CARE DURING WORKING HOURS	14008	14-8
END-OF-DAY SECURITY CHECKS	14009	14-9
SAFEGUARDING DURING VISITS	14010	14-10
SAFEGUARDING DURING CLASSIFIED MEETINGS	14011	14-11
REPRODUCTION OF CLASSIFIED MATERIAL .	14012	14-13

FIGURE

14-1	SAMPLE ACTIVITY SECURITY CHECKLIST	14-15
14-2	SAMPLE REPRODUCTION/DISTRIBUTION REQUEST	14-16

MCAS MIRAMAR 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. As classified material, they are official information which must be safeguarded, transmitted and destroyed per this Manual. 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.

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 presence of unauthorized persons.

2. Custodians will not remove classified material from a designated working area except in the performance of official duties and under conditions providing the protection required by reference (b). Under no circumstances will a custodian remove classified material from designated work areas to work on it during off duty hours, or for any other purpose involving personal convenience, without specific approval of the Command Security Manager.

14002. CONTROL MEASURES. Classified information must be afforded a level of accounting and control commensurate with its assigned security classification level. Accounting and control serves to limit dissemination, prevent unnecessary reproduction, and safeguard from unauthorized disclosure.

1. Top Secret. All Top Secret information originated or received by this command will be controlled by the Top Secret Control Officer (TSCO) per the procedures set forth in paragraphs 2-3 and 7-3 of reference (b). Top Secret material will be:

a. Centrally controlled by the CMCC.

b. Assigned a control number and entered into a Top Secret log. This log will include the date originated or received, individual serial numbers, copy number, title, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken.

c. Accounted for by a continuous chain of receipts (hand-to-hand transfer with signed receipts is required), for those documents distributed both internally and externally.

d. Stored in the Command CMCC.

e. Physically sighted at least annually, and more frequently as circumstances warrant (e.g., at change of TSCO).

2. Secret. The proliferation of Secret computer networks, such as the SIPRNET, secure facsimile machines, and other electronic means to receive and transmit Secret information has rendered central control over Secret material impractical. Accordingly, per references (b) and (c), there is no requirement to maintain records of receipt, distribution, or disposition of Secret material. However, administrative provisions are required to protect Secret material from unauthorized disclosure by access control and compliance with the regulations on marking, storage, transmission, and destruction set forth in the references and this Manual. SCP Custodians may implement accountability procedures within the SCP for Secret material.

3. Confidential. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. However, administrative provisions are required to protect Confidential material from unauthorized disclosure by access control and compliance with the regulations on marking, storage, transmission, and destruction set forth in the references and this Manual. SCP Custodians may implement accountability procedures within the SCP for Confidential material.

14003. CLASSIFIED MESSAGES. Messages classified Secret and below are the responsibility of the individual staff section or division receiving them. These messages will be afforded the same level of protection against compromise as standard classified documents. Top Secret messages will be centrally controlled by the TSCO per the procedures set forth in paragraph 14002 above.

14004. SIPRNET E-MAIL AND OTHER ELECTRONICALLY TRANSMITTED MATERIAL. Secret e-mail and attachments or other material obtained from classified computer systems, such as the SIPRNET, and via secure facsimile machines is the responsibility of the individual staff section or division receiving it. Classified information obtained from the SIPRNET must be reviewed to determine proper classification to prevent inadvertent compromise. If information obtained from the SIPRNET is not marked, contact the document's originator to determine the classification of the material. Classified material received via electronic means and printed will be safeguarded commensurate with the highest level of classification in the document.

14005. WORKING PAPERS

1. Working papers such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain Secret or Confidential information will be:

a. Dated when created.

b. Conspicuously marked, centered top and bottom, of 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.
2. If Secret and Confidential working papers are held for over 180 days from date of creation, or officially released outside the command by the originator, they must be controlled and marked in the manner prescribed for a finished document.
 3. If working papers contain Top Secret information, they will be controlled and marked as a finished document per the procedures set forth in reference (b) and paragraph 14002 herein.

14006. SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. Restricted Data (RD) and Formerly Restricted Data (FRD). RD (including CNWDI) and FRD will be controlled and safeguarded per DoD Directive 5210.2, Access to and Dissemination of Restricted Data.
2. Communication Security (COMSEC). COMSEC material is under the accountability and control of the AC/S, G-6 and will be safeguarded per StaO 2601.1, Command Policy for Handling, Accounting and Controlling Communication Security Material System (CMS) Material.
3. SCI. SCI information is controlled and safeguarded by the 3d MAW SSO. Any questions regarding SCI access will be directed to that office.
4. For Official Use Only (FOUO). FOUO information is controlled and safeguarded per SECNAVINST 5720.42E, DON Freedom of Information Act (FOIA) Program. FOUO information will be disposed of by shredding; either strip shredders or cross-cut shredders may be used.
5. Sensitive Unclassified (SU). Sensitive information contained in U.S. Government information systems is controlled and safeguarded per Title 5, Public Law 93-579, The Privacy Act, U.S.C., Section 552a. SU information includes personal data (e.g., medical records, individual financial information, etc.);

privileged data (e.g., chaplain records, safety records, etc.); and proprietary data (e.g., copyrighted material). The unclassified LAN is accredited to process SU information. SU 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 have ever contained.

b. Removable magnetic media, such as removable hard disks, bubble memory boards, etc., will be labeled with a color-coded sticker per paragraph 13003 of this Manual. 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 approved for open storage of classified information, there are no special requirements. 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 Chapter 16 of this Manual.

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. Any personnel who have had disciplinary or behavioral problems will be denied access to the system and to any rooms or compartments containing computers used for classified processing.

c. All personnel entering secure areas to perform maintenance on computers used for classified processing must 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 work spaces, 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 non-government sources is not authorized to process classified information.

14008. CARE DURING WORKING HOURS

1. When classified documents are removed from storage for working purposes, keep them under constant surveillance by an appropriately cleared person at all times. Keep them 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, who will make all appropriate reports and initiate a Preliminary Inquiry per Chapter 18 of this Manual. 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 actions.

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, shown at figure 14-1, will be used for this purpose. A single SF 701 may be employed for interconnected office spaces. Custodians will post the SF 701 on the main entrance door.

2. Those conducting security checks will make sure 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.

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

e. Security alarms and equipment have been activated.

f. Check other items as directed (i.e., STU III phones, power off on shredders, computers, copiers, etc.).

3. All SF 702 forms used to record the opening and locking of security containers, vaults and secure rooms that contain COMSEC information/material will be retained for 2 years. The SF 701 form and all other SF 702 forms will be maintained for 30 days (current month plus previous month).

14010. SAFEGUARDING DURING VISITS. Only visitors with an appropriate clearance level and need-to-know will be granted access to classified information. Refer to Chapter 11 of this Manual for visit procedures.

14011. 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 department/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 (TSCM) Program.

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

e. Attendance will be limited strictly to those persons whose presence is considered necessary in the interests of national security.

4. Departments/staff sections conducting classified meetings at this Station must ensure that:

a. Conference rooms and areas in which classified information is to be discussed afford adequate security against unauthorized access.

b. Adequate storage facilities are available.

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

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

e. 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.

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

g. Classified notes received or taken will be controlled per paragraph 14005 of this Manual.

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

6. Marine Corps and Navy personnel at this Station must have the approval of their Department Head to disclose classified information at meetings conducted by or under security sponsorship of other bases or agencies of the Executive Branch of the Government.

7. When it becomes necessary to provide temporary storage of classified material brought aboard MCAS Miramar after normal working hours, the G-6 Communications Center 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 Miramar during normal working hours, classified material may be stored in the CMCC.

8. Further restrictions and requirements concerning classified meetings are contained in paragraph 7-12 of reference (b).

14012. REPRODUCTION OF CLASSIFIED MATERIAL1. 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.

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, microforms, photographs, slides, and many other formats.

2. Controls on Reproduction

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

(1) Top Secret information will not be reproduced without the consent of the originating activity, higher authority, and the TSCO.

(2) Individuals desiring to reproduce Secret material will obtain authorization from the Command Security Manager or Assistant Security Manager using a Request for Reproduction of Classified Material (Figure 14-2). The Command Security Manager/Assistant Security Manager is responsible for verifying the need to reproduce the classified information, and for ensuring only the minimum required copies are reproduced.

(3) Confidential material may be reproduced in section, division and branch spaces after inspection and approval of their reproduction equipment by the Command Security Manager/Assistant Security Manager.

b. Where possible, two people will be involved in reproducing classified material to ensure positive control and safeguarding of reproduced material. All operators of reproduction equipment authorized for the reproduction of classified information will possess a security clearance at least equivalent to the level of the material being reproduced.

c. If a classified document needs to be reproduced for distribution, the department/staff section concerned will deliver the document to the Command CMCC, along with a Request for Reproduction of Classified Material (Figure 14-2), specifying the document to be reproduced, the control number (if assigned), how many copies to reproduce, the justification, and the distribution. The Assistant Security Manager will check for discrepancies and prepare the reproduced copies for distribution either within the command or outside the command per Chapter 15 of this Manual.

d. The reproduction of classified information may be accomplished only on machines that have been specifically authorized by the Command Security Manager or Assistant Security Manager. All copy machines within this command authorized for reproducing classified material will be posted with a sign reading, for example, "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY (Designated Official)."

e. Copy machines not authorized for the reproduction of classified information will be posted with a warning notice reading, for example, "THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL."

f. 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. Reproduced material on which classification markings are illegible will be remarked by the individual reproducing the material.

g. 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. Areas surrounding reproduction equipment will be checked for classified material that may have been left on nearby desks or thrown in wastebaskets. In the event the machine malfunctions, it will be checked to ensure that all copies have been removed. After reproducing classified material, the machine will be checked to ensure the original and all copies have been removed.

ACTIVITY SECURITY CHECKLIST		Division/Branch	Rank/Name of Div/Sec Security Assistant	Month/Year																									
OFFICIAL STATEMENT of Division/Section official conducting daily security check: I have conducted an end of day physical security examination of the work space(s) indicated, and have checked all the items listed as evidenced by my initials hereon.		Report security threats and vulnerabilities to the Command Security Manager, Bldg 8630, CMCC, Phone 577-8624																											
Work Space/room number(s) included for this checklist:		Additional Remarks:																											
CHECKLIST ITEMS	1	2	3	5	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. GSA Security Containers have been locked, checked, and double checked. (SF 702 Completed).																													
2. Desks and computer workstations have been cleared of all classified information, including magnetic media.																													
3. Windows and doors (when applicable) have been locked.																													
4. Security alarm(s) and equipment have been activated (where applicable).																													
5. Electronic appliances (fans, coffee machines, radios, etc) have been turned off and secured properly.																													
Initials of Division/Section official conducting Daily Security Check																													
Time of Division/Section Security Check of Space/Rooms																													
Initials of CDO/PMO conducting After Hours Security Sweep																													
Time of CDO/PMO After Hours Security Sweep																													
SF 701 (Modified for internal COMCABWEST use only (12-02) (Retain for 30 days following last entry)																													

Figure 14-1. --Sample Activity Security Checklist

MCAS MIRAMAR IPSP

MCAS MIRAMAR IPSP

REQUEST FOR REPRODUCTION OF CLASSIFIED MATERIAL		
SECTION I (REQUEST)		
TO Command Security Manager, Marine Corps Air Station Miramar/Marine Corps Air Bases Western Area Miramar	FROM (DEPT/STAFF SECTION)	DATE
CLASSIFICATION OF MATERIAL (CHECK ONE) CONFIDENTIAL <input type="checkbox"/> SECRET <input type="checkbox"/>	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/RANK OF DIVISION/STAFF SECTION OFFICIAL	SIGNATURE OF DIVISION/STAFF SECTION OFFICIAL	
SECTION II (APPROVAL/DISAPPROVAL)		
FROM Command Security Manager, Marine Corps Air Station Miramar/Marine Corps Air Bases Western Area Miramar	TO (DEPT/STAFF SECTION)	DATE
APPROVED: <input type="checkbox"/>		
DISAPPROVED: <input type="checkbox"/>		
JUSTIFICATION IF DISAPPROVED:		
SIGNATURE OF OFFICIAL APPROVING/DISAPPROVING REQUEST	TITLE OF OFFICIAL	

SAMPLE

Figure 14-2. --Sample Reproduction/Distribution Request

MCAS MIRAMAR IPSP

CHAPTER 15

DISSEMINATION, TRANSMISSION AND TRANSPORTATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	15000	15-3
PREPUBLICATION REVIEW	15001	15-3
DISSEMINATION TO DOD CONTRACTORS	15002	15-4
DISSEMINATION TO FOREIGN GOVERNMENTS	15003	15-4
MAILING CLASSIFIED MATERIAL	15004	15-4
TELEPHONE TRANSMISSION	15005	15-4
RECEIPT FOR CLASSIFIED INFORMATION	15006	15-5
HANDCARRYING CLASSIFIED INFORMATION	15007	15-5
AUTHORIZATION TO HANDCARRY CLASSIFIED INFORMATION IN A TRAVEL STATUS	15008	15-6

FIGURE

15-1	SAMPLE STATEMENT OF UNDERSTANDING FOR ESCORTING OR HANDCARRYING CLASSIFIED INFORMATION.	15-8
------	---	------

MCAS MIRAMAR IPSP

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 Chapter 8 of reference (b).
3. Only appropriately cleared personnel or carriers will transmit, transport, escort, or handcarry classified information, per the provisions of Chapter 9 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 submit all official Marine Corps information proposed for public release to the Command Security Manager for either an interim or final determination as to the releasability of the information.

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 facilities certification of security clearance provided on the classified visit request (see chapter 11 of this Manual), which will be provided to the Command Assistant Security Manager.

15003. DISSEMINATION TO FOREIGN GOVERNMENTS. Authority for disclosure of classified information to foreign governments has been centralized in the Navy International Program Office (IPO), and must be authorized in writing. Foreign visit requests received from the Navy IPO, and approvals/disapprovals to disclose classified information, will be processed via the Command Assistant Security Manager.

15004. MAILING CLASSIFIED MATERIAL. All classified material to be mailed to another activity will be brought to the CMCC. 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. The practice of stating "This is not a secure line" is not a DON requirement. 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) 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. Either 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 CMCC regardless of the method of transmission. Receipts will be maintained for two years.

15007. HANDCARRYING CLASSIFIED INFORMATION

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

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

a. Use a cover sheet or file folder when handcarrying classified information within a building, or between buildings onboard MCAS Miramar.

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

3. When classified information is handcarried 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, barber shop, bowling alley, 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 handcarry classified information either as part of normal duties or in an official travel status. The expiration date on the DD 2501 may not exceed 3 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 local reproduction is prohibited.

6. All personnel handcarrying classified information between the CMCC and a SCP 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 handcarry classified information aboard a U.S. military aircraft. It does not provide sufficient authorization to handcarry classified information aboard commercial aircraft, in which case a courier authorization letter must also be carried by the traveler.

15008. AUTHORIZATION TO HANDCARRY CLASSIFIED INFORMATION IN A TRAVEL STATUS

1. Because of the security risks inherent in handcarrying classified material while in a travel status, it will not be authorized except under extraordinary or emergency circumstances. The widespread use of the SIPRNET makes the need to handcarry classified information while in a travel status almost obsolete. Handcarrying classified information in a travel status will only be authorized under those circumstances described in paragraph 9-11 of reference (b).

2. Requests to handcarry classified material aboard commercial passenger aircraft will be submitted in writing to the Command Security Manager, and will contain the information listed in paragraph 9-13 of reference (b). Upon receipt of the request and the material to be transported, the Command Assistant Security Manager will prepare a courier authorization letter. The designated courier will then personally receipt for the authorization at the CMCC office, building 8630, and receive a briefing on their security responsibilities.

3. All individuals authorized to handcarry 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 Command Security Manager.

4. For additional guidance pertaining to escorting or handcarrying classified information aboard commercial passenger aircraft, refer to paragraph 9-13 of reference (b).

MCAS MIRAMAR IPSP

STATEMENT OF UNDERSTANDING
FOR ESCORTING OR HANDCARRYING CLASSIFIED INFORMATION

I, _____ (Grade, Name, SSN/MOS) _____, hereby certify that I have read and understand my security responsibilities listed below while escorting or handcarrying 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 Miramar 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 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 for Escorting or Handcarrying Classified Information

MCAS MIRAMAR 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 Miramar 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 Miramar 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
CMCC

Figure 15-1. --Statement of Understanding for Escorting or
Handcarrying Classified Information -
Continued

MCAS MIRAMAR IPSP

CHAPTER 16

STORAGE AND DESTRUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	16000	16-3
STORAGE REQUIREMENTS	16001	16-3
ESTABLISHMENT OF CLASSIFIED STORAGE AREAS	16002	16-5
COMBINATIONS	16003	16-6
DESTRUCTION OF CLASSIFIED INFORMATION	16004	16-7
DESTRUCTION METHODS	16005	16-7
DESTRUCTION PROCEDURES	16006	16-8
DESTRUCTION OF UNCLASSIFIED MATERIAL .	16007	16-8

FIGURE

16-1 SAMPLE SECONDARY CONTROL POINT AUTHORIZATION LETTER	16-10
---	-------

MCAS MIRAMAR IPSP

CHAPTER 16

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 Chapter 10 of 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 Command Assistant Security Manager. 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 Chapter 10 of 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) 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 Command Assistant Security Manager 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.

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

6. 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 electro-mechanical 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.

7. The following statement will be attached to the front of all security containers that are not being used for storage of classified information: "THIS CONTAINER NOT USED FOR STORAGE OF CLASSIFIED MATERIAL."

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, located in building 8630, is the primary storage area for classified material addressed to or originated by this command. SCPs are classified storage areas at division and section levels established to facilitate daily access by cognizant personnel. SCPs will be inspected and authorized in writing by the Command Security Manager prior to the storage of classified information within the division or section.

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

a. The applicable department or section head will submit a request for the establishment of a SCP to the Command Security Manager, with a copy to the CMCC. 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 or section head will appoint a primary and alternate custodian in writing for the proposed SCP (see Figure 2-4). A copy of the appointment letters will be forwarded to the CMCC.

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 Manual).

16003. COMBINATIONS

1. Combinations will only be changed by trained personnel. A lockout, as a result of an untrained individual attempting to change a combination, could result in administrative 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 and secure rooms. Combinations will be changed as follows:
 - 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 G-6 Communications Center, 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.
2. Destruction of classified material will be accomplished per Chapter 10 of 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 CMS-1A and CMS-21A. AIS storage media will be declassified or destroyed per NAVSO P-5239-06, 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.

16005. DESTRUCTION METHODS

1. Cross-cut shredders used to destroy classified information must be able to reduce the material to shreds no greater than 3/64 inch wide by 1/2 inch long. Strip shredders will not be used for destruction of classified information.
2. The Command Security Manager/Assistant Security Manager will certify all destruction equipment to be used for destroying classified information. Strip shredders and other shredders in use that do not meet the minimum standards for the destruction of classified information will have the following statement visibly attached to the shredder: "THIS SHREDDER IS NOT AUTHORIZED FOR THE DESTRUCTION OF CLASSIFIED INFORMATION."

3. The primary means of diskette destruction is incineration; however, diskettes may also be degaussed or shredded using a cross-cut shredder.

4. All classified CD ROMs will be returned to the CMCC for destruction using the CD-ROM Destroyer located in the CMCC vault.

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 may be physically destroyed by mutilation or degaussed.

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. Per reference (b), a record of destruction is required for Top Secret and any special types of classified information (see paragraphs 7-7 and 10-17 of reference (b)). Destruction reports will be executed by two witnesses to the destruction and retained for 5 years.

3. Per reference (b), records of destruction are not required for Secret and Confidential information except for special types of classified information. However, when destruction of Secret and Confidential information is conducted at an authorized SCP, the SCP Custodian may record the destruction at their discretion for accountability purposes. The OPNAV 5511/12, "Classified Material Destruction Report" 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 record copies of controlled unclassified information (e.g., FOUO, Sensitive Unclassified, and technical documents assigned distribution statements B through X) per SECNAVINST 5212.5D, Navy and Marine Corps Records Disposition Manual. Non-record copies will be disposed of by shredding, not throwing it 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).

MCAS MIRAMAR IPSP

COMMAND LETTERHEAD

5510
(Originator Code)
(Date)

From: Security Manager, Marine Corps Air Station, Miramar
To: Department/Section Head

Subj: AUTHORIZATION FOR ESTABLISHMENT OF SECONDARY CONTROL
POINT

Ref: (a) Your Request for Authorization dtd _____
(b) Physical Security Survey
(c) SECNAVINST 5510.36
(d) StaO P5510.3

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) and (d).
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:
CMCC

Figure 16-1. -- Sample Secondary Control Point Authorization
Letter

MCAS MIRAMAR IPSP

CHAPTER 17

INDUSTRIAL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	17000	17-3
BACKGROUND	17001	17-3
SECURITY OVERSIGHT OF CLEARED DOD CONTRACTOR OPERATIONS	17002	17-4
CONTRACTING OFFICER'S REPRESENTATIVE (COR)	17003	17-4
VISITS BY CLEARED DOD CONTRACTOR EMPLOYEES	17004	17-5
TRANSMISSION OR TRANSPORTATION	17005	17-5
DISCLOSURE	17006	17-5

MCAS MIRAMAR IPSP

CHAPTER 17

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 Miramar. 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 (NISPOM), 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. DSS, Operations Center Columbus (OCC) grants personnel clearances to individuals in private industry who require access to classified information in order to perform their jobs. The OCC 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 Miramar:

1. Tenant Activities. The DSS 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 DSS OCC, and which have the status of a tenant activity.
2. Visitors. The CG 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 Command Assistant Security Manager, and the department/section where the work will be performed, per Chapter 11 of this Manual. Contractor employees will conform with command security regulations and will be included in the command security education program (see Chapter 4 of this Manual). 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 paragraph 2-6 of 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 paragraph 11-8 of reference (b).

17004. VISITS BY CLEARED DoD CONTRACTOR EMPLOYEES. Cleared contractors planning to visit MCAS Miramar for classified contract work will have their facility security officer submit a visit request in advance, by message or fax, per paragraph 11002 of this Manual. Visit requests handcarried by cleared DoD contractors will not be accepted. Visit requests received by the department/section to be visited will be routed via the Command Assistant Security Manager 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 handcarriers provided that:

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.
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 Manual and Chapter 9 of reference (b).

17006. DISCLOSURE. Refer to Chapter 11 of reference (b) for guidance on disclosing classified information to contractors, including privately-owned or proprietary information, export-controlled technical data, and intelligence information.

MCAS MIRAMAR IPSP

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

CHAPTER 18

	<u>PARAGRAPH</u>	<u>PAGE</u>
DEFINITIONS	18000	18-3
REPORTING RESPONSIBILITIES	18001	18-3
PRELIMINARY INQUIRY (PI)	18002	18-3
ACTIONS TAKEN UPON PI CONCLUSION . . .	18003	18-4
REPORTING LOSSES OR COMPROMISE OF SPECIAL TYPES OF CLASSIFIED INFORMATION AND EQUIPMENT	18004	18-5
JAGMAN INVESTIGATIONS	18005	18-5
PUBLIC MEDIA COMPROMISE	18006	18-6
UNLOCKED SECURITY CONTAINERS	18007	18-6
DISCREPANCIES INVOLVING IMPROPER TRANSMISSIONS	18008	18-7

MCAS MIRAMAR IPSP

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.
3. A possible compromise occurs when classified information is not properly controlled.

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 Chief of Staff will be notified. If circumstances of discovery make such notification impractical, the individual will notify the commanding officer or security manager at the most readily available command or 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 Miramar, and inform the Chief of Staff of the need to initiate a Preliminary Inquiry (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 Chief of Staff 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. Normally, it will be an officer assigned to the department or section having custodial responsibility over the lost or compromised information.

2. PI Submission

a. The PI must be completed within **72** hours, 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 paragraph 12-5 of 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 Chief of Staff 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 paragraph 12-5 and exhibits 12A and 12B of 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 paragraphs 12-4 and 12-8 of 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 Miramar.

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. 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 paragraph 12-8 of 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.

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 Chapter II of JAGINST 5800.7C, 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 Chapter 12 of 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. PUBLIC MEDIA COMPROMISE. A public media compromise is the unofficial release of DoD classified and unclassified information to the public resulting in its unauthorized disclosure. When any individual becomes aware that classified or unclassified information is unofficially released to the public via newspaper, magazine, book, pamphlet, radio, television broadcast, or the INTERNET, they will immediately notify the Command Security Manager or Assistant Security Manager, who will make appropriate notifications per paragraph 12-18 of reference (b). DON personnel will not, under any circumstances, make any statements or comments concerning any information unofficially released to the public.

18007. 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) will immediately contact the custodian of the security container (listed on the SF 700 posted on the interior of the container). The custodian will immediately inventory the contents of the container, vault or secure room to determine if any classified information has been removed (note, however, that this may not be possible to determine under present accountability procedures). The individual finding the unlocked security container will lock the container while waiting for the custodian to arrive.

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/procedures will be taken to prevent future instances from reoccurring.

18008. 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 Assistant Security Manager will notify the forwarding command using OPNAV 5511/51 (Security Discrepancy Notice).