



MASTER DIRECTIVES

UNITED STATES MARINE CORPS

MARINE AIRCRAFT GROUP 12

FIRST MARINE AIRCRAFT WING, MARFORPAC

UNIT 37150

FPO AP 96603-7150

GruO P5510.8A

CMCC -

JAN 09 2000

GROUP ORDER P5510.8A Ch1

From: Commanding Officer
To: Distribution List

Subj: STANDING OPERATING PRODECURES FOR CLASSIFIED MATERIAL
CONTROL CENTER AND SECONDARY CONTROL POINTS OPERATIONS (SHORT
TITLE: SOP FOR CMCC AND SCP OPERATIONS)

Ref: (a) SECNAVINST 5510.36
(b) SECNAVINST 5510.30A
(c) WgO P5510.5D
(d) GruO P5510.6D

Encl: (1) Locator Sheet

1. Purpose. To establish standing operating procedures within Marine Aircraft Group 12 for the Classified Material Control Center and the associated Secondary Control Points.
2. Cancellation. GruO 5510.8
3. Information. This SOP serves as an amplification of the references and sets forth the minimum procedures to be followed within MAG-12 and subordinate units. All units will be guided by the provisions of references (a) through (d) except as modified by this SOP.
4. Summary of Revision. This SOP has been subject to major changes and should be reviewed in its entirety.
5. Recommendation. All recommendations concerning contents of this SOP are invited. Such recommendations are to be forwarded to the Commanding Officer, Marine Aircraft Group 12 (Attn: Security Manager) via the chain of command.
6. Action. Commanding Officers and heads of primary and special staff sections will ensure compliance with the procedures set forth in this order.

GruO-P5510.8A

MAR 09 2000

7. Certification. Reviewed and approved this date.


J. F. FLOCK

DISTRIBUTION: C

MAR 09 2009

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR CLASSIFIED MATERIAL
CONTROL CENTER AND SECONDARY CONTROL POINTS OPERATIONS
(SHORT TITLE: SOP FOR CMCC AND SCP OPERATIONS)

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

ENCLOSURE (1)

UNITED STATES MARINE CORPS

MARINE AIRCRAFT GROUP 12
1ST MARINE AIRCRAFT WING, MARFORPAC
UNIT 37150
FPO AP 96603-7150

GruO P5510.8A Ch 1
CMCC
09 MAR 2001

GROUP ORDER P5510.8A Ch 1

From: Commanding Officer, Marine Aircraft Group 12
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR CLASSIFIED MATERIAL
CONTROL CENTER AND SECONDARY CONTROL POINTS OPERATIONS
(SHORT TITLE: SOP FOR CMCC AND SCP OPERATIONS)

Encl: (1) New page inserts to GruO P5510.8A

1. Purpose. To transmit new page inserts and pen changes to the basic Order.

2. Action

a. Remove Appendix A of the basic Order and replace with corresponding pages contained in the enclosure.

b. The following pen changes are directed:

(1) On page 1-4, para 1005, delete "has designated the MAG-12 Adjutant as the" Replace with - "will designate a"

(2) On page 1-5, para 1007.2 delete "and destroyed material"

(3) On page 1-6, para 1007.5 delete the entire paragraph. Change para 1007.6 to 1007.5

(4) On page 2-4, para 2003.2 delete the entire paragraph, and replace with: "Although there is no requirement under SECNAVINST to maintain accounting records of CONFIDENTIAL material, 1MAW has tasked MAG-12 to account for and control all CONFIDENTIAL material."

(5) On page 2-6, para 2010, delete the entire paragraph. Change para 2011 and 2012 to 2010 and 2011 respectively.

(6) On page 3-4, add para 3000.3 as follows:

3003. The CMCC and SCPs are prohibited from using terms such as 'For Official Use Only' or 'Secret Sensitive' for the identification of classified information.

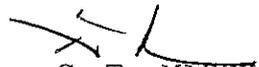
Subj: STANDING OPERATING PROCEDURES FOR CLASSIFIED MATERIAL
CONTROL CENTER AND SECONDARY CONTROL POINTS OPERATIONS
(SHORT TITLE: SOP FOR CMCC AND SCP OPERATIONS)

3. Summary of Changes. These changes reflect updated procedures and compliance with higher directives.

4. Change Notation. Significant changes in the revised pages for this change are denoted by an asterisk (*).

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

6. Certification. Reviewed and approved this date.


G. T. MASCK
Acting

DISTRIBUTION: C

SOP FOR CMCC AND SCP OPERATIONS

CONTENTS

CHAPTER

- 1 PROGRAM MANAGEMENT
- 2 ACCOUNTING AND CONTROL
- 3 CLASSIFICATION AND MARKING
- 4 SAFEGUARDING AND STORAGE
- 5 TRANSMISSION/TRANSPORTATION
- 6 DESTRUCTION

APPENDIX

- A SCP/CMCC INSPECTION CHECKLIST

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 1

PROGRAM MANAGEMENT

	PARAGRAPH	PAGE
BASIC POLICY.....	1000	1-3
AUTHORITY.....	1001	1-3
APPLICABILITY.....	1002	1-3
RESPONSIBILITY.....	1003	1-3
COMMAND SECURITY MANAGER.....	1004	1-4
CLASSIFIED MATERIAL CONTROL CENTER OFFICER..	1005	1-4
CLASSIFIED MATERIAL CONTROL CENTER CUSTODIAN	1006	1-4
SECONDARY CONTROL POINT CUSTODIAN.....	1007	1-5
SECONDARY CONTROL POINT CLERKS.....	1008	1-6
EMERGENCY PLANS/EMERGENCY DESTRUCTION SUPPLEMENT (EP/EDS).....	1009	1-6
INSPECTIONS.....	1010	1-6

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 1

PROGRAM MANAGEMENT

1000. BASIC POLICY. The MAG-12 Classified Material Control Center is established under the authority of the Commanding Officer to ensure the proper transfer, control, and destruction of classified material within the command.

1001. AUTHORITY. The Commanding Officer of MAG-12 is responsible for establishing and maintaining the MAG-12 Classified Material Control Center for the protection and control of classified material.

1002. APPLICABILITY

1. This Order establishes policies for the security of classified material. This Order, in conjunction with the references, will enable the user to implement and maintain an effective classified material control system.
2. The policies and procedures in this Order and its references represent the minimum requirements for all elements of MAG-12. Commanding Officers who feel that more stringent requirements are needed to meet their unique situation will publish their own classified material related directives.
3. Requests for guidance or interpretation of this Order are encouraged. Requests will be addressed by letter or telephone directly to the MAG-12 Security Manager or the MAG-12 Classified Material Control Center Officer.
4. This Headquarters will publish, as circumstances dictate, memorandums that interpret official policy. These memorandums will be based on questions raised within MAG-12 elements and directives issued by higher headquarters.

1003. RESPONSIBILITY

1. Commanding Officers are responsible for compliance with this Order within their squadrons/detachments.
2. All MAG-12 personnel are responsible for compliance with

this Order.

1004. COMMAND SECURITY MANAGER. The Commanding Officer of MAG-12 has designated the MAG-12 Executive Officer as the Security Manager. The Security Manager is responsible for the overall management of the information security program, including the establishment of the Classified Material Control Center. The Security Manager has delegated the performance of the duties pertaining to the CMCC to the CMCC Officer.

1005. CLASSIFIED MATERIAL CONTROL CENTER OFFICER. The Commanding Officer ~~has designated the MAG-12 Adjutant as the~~ "will designate a" Classified Material Control Center Officer responsible to the Security Manager for overall handling, control, dissemination, and destruction of classified material within the command. The CMCC Officer must ensure references (a) through (d) are on hand and current. The duties of the CMCC Officer are (but not restricted to) the following:

1. Maintain a folder of each SCP that contains all relevant information (e.g., appointment letters, physical security evaluations, destruction reports, inventories, access rosters, etc.).
2. Maintain a master inventory of all documents held in the CMCC and its SCPs.
3. Provide inventory printouts to the SCPs on the occasions that inventories are required.
4. Indoctrinate all newly appointed SCP custodians and provide on-going refresher training to all custodians and clerical personnel.
5. Provide assistance to the SCPs as necessary to maintain proper accountability of all classified material.
6. Advise the Security Manager of any irregularities within the SCPs of the CMCC.

1006. CLASSIFIED MATERIAL CONTROL CENTER CUSTODIAN. The CMCC custodian will be appointed in writing and will be guided by the references of this Order. The duties of the CMCC custodian are (but not limited to) the following:

1. Manage the day to day operations of the CMCC.
2. Conduct inspections/inventories of the MAG-12 SCPs when directed by the CMCC Officer.
3. Conduct all duties of the CMCC Officer when he/she is not available.
4. Ensure all access rosters within MAG-12 SCPs and CMCCs are current.

1007. SECONDARY CONTROL POINT CUSTODIAN. A Secondary Control Point is established to permit storage of classified material at a location outside the CMCC to serve the needs of the organization. A SCP may only draw classified material from one source, which is the parent CMCC. When the need for a SCP no longer exists, the material contained therein will be returned to the CMCC and the SCP disestablished. The Commanding Officer has determined that there are two SCPs located within the MAG-12 Headquarters. The custodian of each will be an Officer who will normally be present to supervise the operation of the SCP. All personnel assigned to the SCP must have a security clearance commensurate with the level of material held in the SCP. They are: SCP A, in MAG-12 S-2; and SCP B, in MAG-12 S-3. Each of the SCPs is required to designate in writing a Secondary Control Point Custodian. The SCP Custodians' duties and responsibilities are (but not limited to) the following:

1. Be thoroughly familiar with the contents of this Order. Upon appointment, the new SCP Custodian will report to the CMCC Officer to be briefed on the functioning of the SCP.
2. Oversee the daily operation of the designated SCP, including accounting for newly received ~~and destroyed material~~, access control of personnel within the SCP, maintenance of logbooks and control forms as indicated in the enclosure, and continual review of holdings to maintain only the minimal material needed to conduct operations.
3. Designate in writing any clerical personnel who will be working in the SCP, those personnel who are authorized to receipt for material for the SCP, and those personnel who are authorized access to the SCP. Each SCP will be designated in writing and will have the Group S-2 complete a Physical Security

Evaluation.

4. Conduct an inventory of holdings upon assumption or relief of appointment, semiannually, and whenever directed. The SCP Custodian will verify all inventories conducted. Any discrepancies will be reported to the Security Manager via the CMCC Officer.

~~5. Authorize destruction of SCP held material~~

5. Maintain an emergency plan/emergency destruction supplement for the SCP and test this plan at least annually. Maintain a written report of such test. The Custodian will ensure that the CMCC Officer receives a copy of all EP/EDS drills conducted.

1008. SECONDARY CONTROL POINT CLERKS. SCP clerks may be assigned but must be Lance Corporals or above. All Personnel assigned to the SCP must have a security clearance commensurate with the level of material held in the SCP.

1. Upon appointment, the new SCP Clerk will report to the SCP Custodian to be briefed on the functioning of the SCP.

2. Maintain the daily operation of the designated SCP. This includes accounting for newly received and destroyed material, access control of personnel within the SCP, maintenance of logbooks and control forms as indicated in the enclosure, and continual review of holdings to maintain only the minimal material needed to conduct operations.

3. The SCP Clerk will recommend destruction of unnecessary classified material to the SCP Custodian. (Any material to be destroyed will be turned in the CMCC for destruction. The SCP will not destroy any controlled items/material itself.)

1009. EMERGENCY PLANS/EMERGENCY DESTRUCTION SUPPLEMENT (EP/EDS). All MAG-12 squadrons/detachments that handle classified information will develop emergency plans. In developing these plans and procedures, consideration will be given to both tactical and garrison environments. Review Reference (b) on requirements and format for EP/EDS.

1010. INSPECTIONS. All permanent squadrons under MAG-12 will receive an annual Functional Area Inspection (FAI) for the CMCC

by the Assistant Security Manager, 1st MAW, G-2. MAG-12 will also complete a semiannual review of all CMCCs and SCPs within the Group in the months of June and December. This review will be accomplished by using the 1st MAW inspection checklist located in Appendix A. UDP squadrons will be inspected once during their UDP cycle. Any MAG-12 subordinate element may request a Staff Assistance Visit (SAV) from the MAG-12 Security Manager at any time.

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 2

ACCOUNTING AND CONTROL

	PARAGRAPH	PAGE
BASIC POLICY.....	2000	2-3
INVENTORY.....	2001	2-3
REVIEW OF DOCUMENTS.....	2002	2-3
CONFIDENTIAL.....	2003	2-4
SECRET.....	2004	2-4
TOP SECRET.....	2005	2-5
CLASSIFIED MESSAGES.....	2006	2-5
WORKING PAPERS.....	2007	2-5
MAIL HANDLING.....	2008	2-5
SECRET CONTROL.....	2009	2-5
CONFIDENTIAL CONTROL.....	2010	2-6
PHYSICAL SECURITY.....	2011	2-6
CLASSIFIED MATERIAL REVIEW BOARD.....	2012	2-6

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 2

ACCOUNTING AND CONTROL

2000. BASIC POLICY. Classified Material Control Centers (CMCCs) and Secondary Control Points (SCPs) are the instruments through which organizations and staff sections of MAG-12 will exercise accountability and control over classified documents and materials. Commanders will ensure that all classified holdings are reduced to the absolute essentials required for mission accomplishment.

2001. INVENTORY. CMCC/SCP inventories will be conducted upon change of custodians, whenever a loss or suspected loss of material has occurred, and at least semiannually during the months of December and June. UDP squadrons will conduct a complete inventory upon arrival and prior to departure from MCAS Iwakuni. Inventory results will be submitted to the MAG-12 Security Manager via the MAG-12 CMCC. Inventories will be accomplished in the following manner:

1. Obtain a master control inventory from the CMCC.
2. Compare all documents listed on that inventory with all documents on hand. Add any documents that are not listed. Annotate the destruction number, transfer number, or other supporting evidence to explain numbers listed but not on hand.
3. Compare the current inventory with the previous inventory to ensure that all documents are accounted for. Ensure all the documents listed on the previous inventory that are not listed on the new inventory are properly accounted for.
4. The completed inventory will be returned to the CMCC and reconciled with records in the CMCC within five working days of its submission.
5. Any discrepancies will be reported to the MAG-12 Security Manager via CMCC Officer.

2002. REVIEW OF DOCUMENTS. The SCP custodian will review the material held in order to verify its need. Material no longer needed or declassified will be turned into the CMCC for destruction. The goal is to retain the minimum amount of

classified material commensurate with the needs of the unit.

2003. CONFIDENTIAL. The following policies pertain to the protection of CONFIDENTIAL material:

1. The material at all times will be safeguarded from unauthorized disclosure.
2. ~~There is no requirement to maintain accounting records of CONFIDENTIAL material. On receipt of CONFIDENTIAL material, the material will be processed through the CMCC to ensure proper control at all times. The SCP custodian will maintain the material on inventory, but will not have an assigned control number. Additionally, the SCP will ensure all appropriate marking and storing requirements are fulfilled.~~ *Although there is no requirement under SECRET/CONFIDENTIAL, IMAW has tasked MAG-1d to account for and control all CONFIDENTIAL material.*

2004. SECRET. The following policies pertain to the protection of SECRET material excluding messages, which are not accounted for except as in paragraph 2006:

1. The material will be safeguarded at all times from unauthorized disclosure.
2. SECRET material will be accounted for in the following manner:
 - a. All SECRET material will be checked into the CMCC to ensure proper control and accounting of the document/material.
 - b. Once the CMCC has logged in the material to its logbook/database, the appropriate SCP will be notified they have received classified material.
 - c. The SCP will inspect the material to ensure it is required and the representative will sign for the material. Both the CMCC and the SCP will ensure that the new material is entered into their individual databases/inventories.
3. Accounting records such as receipts and destruction reports will be maintained in a clear and legible manner for at least two years after the material is no longer maintained or downgraded.
 - a. Destruction of SECRET material must be documented by one witness who physically observes the destruction of the

material. Destruction will be reported using the CMCC database destruction report format along with cover letter.

b. NATO SECRET messages kept over 90 days will be accounted for and destroyed using the above procedures.

2005. TOP SECRET. The CMCC is not authorized to control/store TOP SECRET material. If there is an instance where TOP SECRET information is received in the CMCC, it is to be turned over to the TOP SECRET Control Officer.

2006. CLASSIFIED MESSAGES. Classified messages can be maintained for a maximum of 90 days. After that time, they must either be destroyed or assigned a control number and treated as a document. A group of similar messages may be filed in a common folder under a single control number. SECRET messages are accounted for in the CMCC Message Logbook.

2007. WORKING PAPERS. Working papers are the unfinished materials created in the process of making a classified document. Working papers must be stamped the date they were created, marked with the highest classification of the material contained therein, and must have a destruction date on the front of the document. Within 180 days of origination they must either be controlled with a control number from the CMCC or they must be destroyed.

2008. MAIL HANDLING. All certified and registered mail received by MAG-12 will be turned into the CMCC unopened. Return receipts will be processed within 24 hours upon receipt.

2009. SECRET CONTROL

1. Upon receiving material without a return receipt card enclosed, an OPNAV Form 5511/10 will be filled out and returned to the originator.

2. Material sent from one CMCC to another will have the original sheet of the record of receipt attached. The receipt will be signed, dated, and returned to originating CMCC. This procedure will provide a chain of custody for each document.

3. The originating CMCC will file the document custody card or record of receipt in a separate file.

4. MAG-12 uses both a logbook and database as an accounting system. Each copy of material received will have an entry. The following information will be recorded for each classified document:

- a. Initial control number.
- b. Group/squadron CMCC number.
- c. Registered mail number.
- d. Originator of the material.
- e. Date of the document.
- f. Copy number.
- g. Date received.
- h. Unclassified title.
- i. Downgrading instructions.

5. All material will have the CMCC control number, date received, and copy number stamped on the cover.

~~2010. CONFIDENTIAL CONTROL. Procedures for the protection of CONFIDENTIAL material are less stringent than those for SECRET; there is no requirement for maintaining records of receipt, distribution, or disposition. Holding of CONFIDENTIAL material must be maintained on the unit's inventory but does not require a CMCC control number.~~

¹⁰
2011. PHYSICAL SECURITY. CMCCs and SCPs must meet the physical security standards as set forth in the references. CMCCs and SCPs will establish screening points to ensure that all incoming classified material is properly controlled and access is limited to appropriately cleared personnel.

¹¹
2012. CLASSIFIED MATERIAL REVIEW BOARD. Classified material stored within a CMCC/SCP will be periodically reviewed to ensure its retention is still valid. A review board will be conducted semiannually in June and December, with the results documented and maintained by the CMCC for at least two years. Commands will review classified message traffic quarterly to ensure their

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 3

CLASSIFICATION AND MARKING

	PARAGRAPH	PAGE
CLASSIFICATION.....	3000	3-3
DECLASSIFICATION.....	3001	3-3
MARKING.....	3002	3-4

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 3

CLASSIFICATION AND MARKING

3000. CLASSIFICATION

1. Per reference (c), the Commanding General is the only person within 1st MAW with original classification authority. MAG-12 has been granted derivative authority to create classified material based on the inclusion of material from other classified sources. Derivative classification is the incorporating, paraphrasing, restating, or generating in a new form information that is already classified. There are several items that a derivative classifier must be aware of:

a. Observe and respect the original classification determinations made by the Original Classification Authorities (OCAs).

b. All information derived from a classified document will be marked with the same classification as on the source document. Carry forward from the source document to any newly created document, the appropriate classification markings.

2. Individuals within MAG-12 who believe that the information contained in a document is classified may assign a tentative classification to the document. Safeguard the information according to the believed classification, mark it as "TENTATIVE SECRET (or CONFIDENTIAL)", and forward it up the chain of command for a determination of the appropriate classification.

3001. DECLASSIFICATION. MAG-12 personnel are not authorized to downgrade, declassify, or modify information. However, the authority to downgrade, declassify, or modify is not to be confused with the responsibility of an authorized holder of the classified information to downgrade, declassify, or modify it as directed by classification guidance or the relevant OCA.

3002. MARKING

1. All classified material will be marked clearly with the date and office of origin, the appropriate classification level, and all required "associated markings". These "associated markings" include: the source of classification, downgrading and

declassification instructions, and any appropriate warning notices/markings.

2. Classified material refers to any product that contains classified material regardless of form. This includes paper, AIS media, recordings, photographs, and electronic messages.

3. Classified documents will show its overall classification on the cover, on the title page, and on each interior page. *The CMCC and SCPs are prohibited from using terms such as 'For Official Use Only' or 'Secret Sensitive' for the identification of classified information.*

4. Classified information provided to MAG-12 by a foreign government or an international organization will be assigned a classification that assures equivalent protection.

5. When marking derivatively classified documents, ensure the face of the document contains a "Derived From" line with the source document identified. If using more than one source document, place "Multiple Sources" on the "Derived From" line. Additionally, the originator of the new document must maintain a record of the sources on or with the file or record copy of the document. The list of sources used will be maintained at the back of the derived document.

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 4

SAFEGUARDING AND STORAGE

	PARAGRAPH	PAGE
BASIC POLICY.....	4000	4-3
SAFEGUARDING.....	4001	4-3
STORAGE.....	4002	4-3
COMBINATIONS.....	4003	4-4

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 4

SAFEGUARDING AND STORAGE

4000. BASIC POLICY. Classified material will be used within designated secure areas that will prevent its unauthorized disclosure. All office spaces within the MAG-12 Headquarters and Building 1400 (CONAD/Supply/NBC) are authorized to work with classified material. However, it is essential that the material be protected per reference (a). When material is not being used, it must be stored in an approved area (i.e. SCP or CMCC).

4001. SAFEGUARDING. In addition to the procedures in reference (d), there are other steps needed to ensure proper safeguarding of classified material:

1. Keep classified information under constant surveillance by authorized personnel or covered with SFs 703, 704, or 705.

2. When transporting classified information between offices within the MAG-12 Headquarters complex, ensure the information is secured in a folder or binder marked with the appropriate classification (SF 703, 704, or 705).

3. Outside the MAG-12 HQ Complex (i.e. NBC/CONAD/Supply) or elsewhere, classified material will be double wrapped. A briefcase may serve as the outer wrapping.

4. When in a mixed working environment (classified and unclassified) AIS media shall be marked with an SF 706, 707, 708, or 710 as applicable.

5. To help distinguish between classified and unclassified information, all classified information generated from electronic media at MAG-12 will be printed on yellow paper. Classified photographs can be printed on white paper to facilitate ease of viewing. Regardless of paper color all classified material must be properly marked per reference (a).

4002. STORAGE. Classified material will be stored in the manner prescribed in Chapter 10 of reference (a).

1. The CMCC and individual SCPs will maintain the security container record form (OPNAV 5510/21) for each container.

2. Classified material will not be removed from designated work areas for work at home without prior approval of the MAG-12 Security Manager.

3. Only classified material will be kept in classified material containers.

4003. COMBINATIONS. Combinations to security containers, vault doors, and strong rooms will be changed when the locks are first placed in use, been subject to compromise, when an individual knowing the combination(s) no longer requires access, or when the container is taken out of service. In addition, all combinations will be changed on an annual basis. Combinations will be changed and recorded on a security container information form (SF 700). This sealed form will be assigned the highest level of classification of the material stored within the container. The parent CMCC will store SCP combinations. Squadron CMCC combinations will be stored by the MAG-12 CMCC. MAG-12 CMCC will store its combinations within the 3rd SSCT.

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 5

TRANSMISSION AND TRANSPORTATION

	PARAGRAPH	PAGE
BASIC POLICY.....	5000	5-3
MAILING OF CLASSIFIED MATERIAL.....	5001	5-3
RECEIVING CLASSIFIED MAIL	5002	5-3
HANDCARRYING CLASSIFIED MATERIAL.....	5003	5-4

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 5

TRANSMISSION AND TRANSPORTATION

5000. BASIC POLICY. Only cleared personnel who are designated couriers are authorized to transmit, transport, escort, or handcarry classified information per Chapter 9 of reference (a).

5001. MAILING OF CLASSIFIED MATERIAL. On MCAS Iwakuni, all classified material is sent via registered mail. Currently this is the only method authorized to receive and send classified material to/from FPO addresses. All classified material will be delivered to the CMCC for mailing. Prior to transmitting classified material, the following steps will be taken by CMCC personnel:

1. Enter the material into the inventory.
2. Prepare a list of what will be transmitted and to whom.
3. Use the double wrap system. The outer wrapping will be sealed with heavy-duty paper tape or reinforced nylon tape. The inner wrapper will have the classification of the contained information on its outside.
4. Ensure no classified text is in direct contact with the inner envelope or container.
5. Address the outer envelope or container to an official U. S. Government activity or a cleared DoD contractor. The classified information will not be addressed to an individual; however, an attention line may be used to include a specific department to assist in internal routing.
6. Attach a Record of Receipt (OPNAV Form 5511/10) to the inner wrapper of the classified material. If this receipt is not returned to the sending party, then the originator will start tracer action. Retain all Records of Receipt for two years.

5002. RECEIVING CLASSIFIED MAIL. Acknowledging receipt of classified information is required to ensure that a possible loss or compromise will not occur. The OPNAV 5511/10 must be returned within 24 hours after receipt.

5003. HANDCARRYING CLASSIFIED MATERIAL

1. Handcarrying classified material off-base by personnel in a travel status will not be authorized except in exceptional and approved cases that are absolutely essential to mission accomplishment. Handcarrying will be done by individuals with the appropriate clearance, having in their possession an authorized Courier Card. The Courier Cards are maintained and controlled by the MAG-12 CMCC.
2. Sections/Individuals desiring courier cards will submit written requests to the MAG-12 CMCC through their chain of command via the MAG-12 Security Manager. The request will include the following information: name, rank, unit, sex, race, height, weight, age, hair color, eye color, SSN, RTD, and justification. This information will be transferred to the Courier Authorization Card (DD Form 2501) and will be signed by either the MAG-12 Security Manager or the Assistant Security Manager.
3. The transportation of classified material aboard commercial aircraft outside CONUS is forbidden without the written prior approval of Commanding General, Fleet Marine Force, Pacific. Requests for authorization will be forwarded via the Wing Security Manager. If approved, the courier must comply with the accountability and security standards outlined in reference (a).

SOP FOR CMCC AND SCP OPERATIONS

CHAPTER 6

DESTRUCTION

6000. BASIC POLICY. MAG-12 units will use the current editions of references (a) and (d) as guides for the proper destruction of classified material. All official unclassified material originated within MAG-12 will be shredded or burned. Under no circumstances will classified or unclassified material be placed in trashcans. Trashcans will hold only trash (i.e. soda cans, gum wrappers, etc.). Unclassified publications are not required to be destroyed. Questions and requests for waivers concerning the destruction of official unclassified material should be directed to the MAG-12 Security Manager.

6001. ACCOUNTABLE MATERIAL. Each unit/squadron CMCC is responsible for the destruction of all classified material held within their unit/squadron. When destroying classified material, the MAG-12 CMCC database destruction report will be the primary means used for record purposes and maintained on file for two years. If a subordinate unit/squadron does not use a database, they must produce a destruction report (OPNAV 5511/12) with the following information:

1. CMCC Control Number.
2. Long Title.
3. Copy number.
4. Destruction date.
5. Document classification.

6002. NON-ACCOUNTABLE MATERIAL. Material never entered into the CMCC control system (i.e. working papers, classified waste, etc.) will be destroyed without the need for a destruction report. While awaiting destruction, it will be afforded the protection of classified material of a commensurate level.

6003. METHODS OF DESTRUCTION

1. Whenever classified material is destroyed, it is the CMCC custodian's responsibility to ensure the destruction is complete and thorough.

2. Destruction resources available to MAG-12 units include the cross cut shredders at the MAG-12 CMCC, S-2, and S-3. An incinerator located at the Station Communication Center is also available for use by MAG-12 personnel.

3. Paper products can be burned in approved burn-barrels or destroyed in shredders that crosscut to 1/32 inch. Plastic or synthetic material is to be burned in approved burn-barrels. Microfiche, videos, backup tapes, and 3 1/2 inch disks can either be shredded or burned.

4. MAG-12 units cannot destroy CD-ROM media. This media will be prepared for transmission per Chapter 9 of reference (a).

5. Secret and Confidential material requires only one individual to witness destruction. NATO information will be destroyed per Chapter 10 of reference (a). Any question as to what measures to take in destruction of classified material is to be directed to the Assistant Security Manager.

6004. SQUADRON CMCC DESTRUCTION REPORTS. Squadron CMCCs will complete an original and one copy of every destruction report. The original will be submitted to the MAG-12 CMCC and the copy will be filed when appropriate action is completed. SCPs will not destroy classified material but will return the items for destruction to the parent CMCC.

CLASSIFIED MATERIAL CONTROL CENTER (CMCC) (270)

(REVISED 000710)

Appendix A

UNIT: _____ DATE INSP: _____
 CMCC CUSTODIAN: _____ DATE ASGD: _____
 CMCC OFFICER: _____ DATE ASGD: _____

INTRODUCTION TO THE ISP

	YES	NO	N/A
1. Does the command hold the current edition of SECNAVINST 5510.36? (SECNAVINST 5510.36, 1-1)	___	___	___
2. Is the command in possession of the following classified information references: (SECNAVINST 5510.36,1-1)	___	___	___
a. NATO, OPNAVINST C5510.101D?	___	___	___
b. Classified information released to industry, NISPOM?	___	___	___
c. Controlled unclassified information, DoD 5200.1-R?	___	___	___
3. Are waivers and exceptions submitted to the CNO (N09N2) for all conditions that prevent compliance with SECNAVINST 5510.36? (SECNAVINST 5510.36,1-2)	___	___	___

COMMAND SECURITY MANAGEMENT

1. Has the commanding officer: (SECNAVINST 5510.36,2-1)			
a. Issued a command security instruction?	___	___	___
b. Approved an emergency plan for the protection and destruction of classified information ?	___	___	___
c. Established an Industrial Security Program?	___	___	___
d. Ensured that the security manager and other personnel have received security education and training?	___	___	___
e. Ensured that personnel are evaluated on the handling, creation or management of classified information on performance evaluations?	___	___	___
2. To implement the ISP, has the commanding officer designated in writing a command?			
a. Security Manager? (SECNAVINST 5510.36,2-2)	___	___	___
b. TSCO? (SECNAVINST 5510.36,2-3)	___	___	___
c. TSCA? (SECNAVINST 5510.36,2-3)	___	___	___
d. Assistant Security Manager? (SECNAVINST 5510.36,2-4)	___	___	___
e. Security Assistant? (SECNAVINST 5510.36,2-4)	___	___	___
f. NATO Control Officer and alternate? (SECNAVINST 5510.36,2-5)	___	___	___

3. Has the command security manager:
(SECNAVINST 5510.36, 2-2)
- a. Developed a command security instruction? _____
 - b. Formulated, coordinated, and conducted a command security education program? _____
 - c. Kept command personnel abreast of all changes in security policies and procedures? _____
 - d. Reported and investigated all security threats and compromises? _____
 - e. Promptly referred all incidents, under their jurisdiction, to the NCIS? _____
 - f. Coordinated the preparation of the command SCGS? _____
 - g. Maintained liaison with the PAO on proposed media releases? _____
 - h. Developed security procedures for visitors who require access to classified information? _____
 - i. Implemented regulations concerning the disclosure of classified information to foreign nationals? _____
4. Does the TSCO manage and control all command TS information, less SCI? (SECNAVINST 5510.36,2-3) _____
5. Are security functions performed by another command covered by a written SSA? (SECNAVINST 5510.36, 2-10) _____

SECURITY EDUCATION

- 1. Does the command have an effective information security education program? (SECNAVINST 5510.36,3-1) _____
- 2. Is additional ISP training provided to? (SECNAVINST 5510.36, 3-3) _____
 - a. Derivative classifiers, security managers, and other security personnel? _____
 - b. Classified couriers? _____
 - c. Declassification authorities? _____

CLASSIFICATION MANAGEMENT

- 1. Is information classified only to protect NSI? (SECNAVINST 5510.36, 4-1) _____
- 2. Do procedures prohibit the use of terms such as "For Official Use Only" or "Secret Sensitive" for the identification of classified information? (SECNAVINST 5510.36, 4-2) _____
- 3. Is information, not officially released or disclosed to the public, classified or reclassified only if the information meets the criteria of E.O. 12958? (SECNAVINST 5510.36, 4-11) _____

4. Is the classification level, of any information believed to be improperly classified, challenged? (SECNAVINST 5510.36,4 -12) ___ ___ ___
5. Does NATO and FGI retain its original classification level and is it assigned an English classification equivalent, if necessary? (SECNAVINST 5510.36, 4-17 & 6-14) ___ ___ ___
6. Are procedures established for the completion of command mandatory declassification reviews within 45 working days? (SECNAVINST 5510.36, 4-23) ___ ___ ___
7. Are reasonable steps taken to declassify information determined to be of permanent historical value prior to their accession into NARA? (SECNAVINST 5510.36, 4-25) ___ ___ ___

MARKING

1. Are classified documents and their portions properly marked to include all applicable basic and associated markings? (SECNAVINST 5510.36, 6-1, 6-5) ___ ___ ___
2. Are originally classified documents marked with a "Classified by" and "Reason" line? (SECNAVINST 5510.36, 6-8) ___ ___ ___
3. Are derivatively classified documents marked with a "Derived from" line? (SECNAVINST 5510.36, 6-9) ___ ___ ___
4. Is "Multiple Sources" annotated on the "Derived from line of classified documents derived from more than one source? (SECNAVINST 5510.36, 6-9) ___ ___ ___
5. Is a source listing attached to the file copy of all documents classified by "Multiple Sources?" (SECNAVINST 5510.36, 6-9) ___ ___ ___
6. Are downgrading and declassification instructions included on all classified documents, less exception documents? (SECNAVINST 5510.36, 6-10) ___ ___ ___
7. Are the appropriate warning notices placed on the face of classified documents? (SECNAVINST 5510.36, 6-11) ___ ___ ___
 - a. Overall classification ___ ___ ___
 - b. Declassification date ___ ___ ___
 - c. Date of origination ___ ___ ___
8. Are classified intelligence documents/portions marked with the appropriate intelligence control marking(s)? (SECNAVINST 5510.36, 6-12) ___ ___ ___
9. Are the portions of documents containing NATO and FGI marked to indicate their country of origin? (SECNAVINST 5510.36, 6-14) ___ ___ ___

10. Is the face of NATO and foreign government restricted documents and FGI marked with the appropriate notice? (SECNAVINST 5510.36, 6-15) _____
11. Is the assignment and use of nicknames, exercise terms, and code words per OPNAVINST 5511.37C? (SECNAVINST 5510.36, 6-17) _____
12. Is an explanatory statement included on the face of documents classified by compilation? (SECNAVINST 5510.36, 6-18) _____
13. Do documents, marked classified for training and test purpose, include a statement indicating that the documents are actually unclassified? (SECNAVINST 5510.36, 6-20) _____
14. When removed or used separately, are component parts of classified documents marked as separate documents? (SECNAVINST 5510.36, 6-21) _____
15. Are letters of transmittal marked to show the highest overall classification level of any information being attached or enclosed? (SECNAVINST 5510.36, 6-24) _____
16. Are electronically transmitted messages properly marked? (SECNAVINST 5510.36, 6-25) _____
17. Are classified files or folders marked or have the appropriate SFs been attached to indicate the highest overall classification level of the information contained therein? (SECNAVINST 5510.36, 6-26) _____
18. Are all classified materials, such as AIS media, maps, charts, graphs, photographs, slides, recordings, and videotapes appropriately marked? (SECNAVINST 5510.36, 6-27 through 6-34) _____

SAFEGUARDING

1. Does the command ensure that all DON employees (military and civilian) who resign, retire, separate, or are released from active duty, return all classified information in their possession? (SECNAVINST 5510.36, 7-1) _____
2. Does the command have control measures in place for the receipt and dispatch of Secret information? (SECNAVINST 5510.36, 7-4) _____
3. Are control measures in place to protect unauthorized access to command TS, Secret, or Confidential information? (SECNAVINST 5510.36, 7-3, 7-4, 7-5) _____
4. Are working papers: (SECNAVINST 5510.36, 7-6)
 - a. Dated when created? _____
 - b. Marked "Working Paper" on the first page? _____

- c. Marked with the highest overall classification, center top and bottom, of each applicable page? _____
 - d. Destroyed when no longer needed? _____
 - e. Brought under accountability after 180 days or when they are released outside the command? _____
5. Are appropriate control measures taken for other special types of classified information? (SECNAVINST 5510.36, 7-7) _____
 6. Are SFS 703, 704, and 705 placed on all classified information when removed from secure storage? (SECNAVINST 5510.36, 7-9) _____
 - a. Are SFS 706, 707, 708, and 712 being utilized on all classified AIS media? _____
 - b. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level? _____
 7. Has the command established procedures for end of day security checks, to include the use of SFS 701 and 702? (SECNAVINST 5510.36, 7-10) _____
 8. Are classified vaults, secure rooms, and containers made an integral part of the end of day security check? (SECNAVINST 5510.36, 7-10) _____
 9. Are procedures in place to ensure that visitors have access only to information for which they have a need-to-know and the appropriate clearance level? (SECNAVINST 5510.36, 7-11) _____
 10. Are procedures in place for classified meetings held at the command or hosted at cleared facilities? (SECNAVINST 5510.36, 7-12) _____
 11. Is classified information reproduced only to the extent that is mission essential? (SECNAVINST 5510.36, 7-13) _____

DISSEMINATION

1. Are special types of classified and controlled unclassified information disseminated per their governing instructions? (SECNAVINST 5510.36, 8-4) _____
2. Is command information intended for public release, including information released through AIS means (i.e., INTERNET, computer servers) submitted for prepublication review? (SECNAVINST 5510.36, 8-8) _____

TRANSMISSION AND TRANSPORTATION

- 1. Is classified information transmitted and transported only per specific requirements? (SECNAVINST 5510.36, 9-2, 9-3, 9-4) _____
- 2. Are special types of classified information transmitted and transported per their governing instructions? (SECNAVINST 5510.36, 9-5) _____
- 3. Are command personnel advised not to discuss classified information over unsecured circuits? (SECNAVINST 5510.36, 9-6) _____
- 4. Are command procedures established for preparing classified bulky shipments as freight? (SECNAVINST 5510.36, 9-7) _____
- 5. Is classified information transported or transmitted outside the command receipted for? (SECNAVINST 5510.36, 9-10) _____
- 6. Does the command authorize the handcarry or escort of classified information, via commercial aircraft, only if other means are not available, and there is an operational need or contractual requirement? (SECNAVINST 5510.36, 9-11) _____
- 7. Are designated couriers briefed on their courier responsibilities and requirements? (SECNAVINST 5510.36, 9-11) _____
- 8. Are procedures established for the control and issuance of the DD 2501? (SECNAVINST 5510.36, 9-12) _____

STORAGE AND DESTRUCTION

- 1. Are any command weaknesses, deficiencies, or vulnerabilities in any equipment used to safeguard classified information reported to the CNO (N09N3)? (SECNAVINST 5510.36, 10-1) _____
 - a. Does the command ensure that weapons, money, jewelry or narcotics are not stored in security containers used to store classified information? _____
 - b. Does the command ensure that external markings on command security containers do not reveal the level of information stored therein? _____
- 2. Does command security equipment meet the minimum standards of GSA? (SECNAVINST 5510.36, 10-2) _____
- 3. Does the command meet the requirements for the storage of classified bulky information? (SECNAVINST 5510.36, 10-3) _____

4. Does the command mailroom have a GSA-approved security container to store USPS first class, certified, and registered mail overnight?
(SECNAVINST 5510.36, 10-3) _____
5. Are command vaults and secure rooms, not under visual control at all times during duty hours, equipped with electric, mechanical, or electro-mechanical access control devices?
(SECNAVINST 5510.36, 10-7) _____
6. Are specialized security containers securely fastened to the structure, rendering them non-portable? (SECNAVINST 5510.36, 10-8) _____
7. Has the command removed all containers manufactured by Remington Rand?
(SECNAVINST 5510.36, 10-9) _____
8. Is classified information removed from designated work areas for work at home done so only with prior approval of appropriate officials? (SECNAVINST 5510.36, 10-10) _____
9. Are command container combinations changed:
(SECNAVINST 5510.36, 10-12)
 - a. By individuals who possess the appropriate clearance level? _____
 - b. Whenever the container is first put into use? _____
 - c. Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)? _____
 - d. Whenever a combination has been subjected to compromise? _____
 - e. Whenever the container is taken out of service? _____
10. Are command container combinations marked, and accounted for per the classification level of the information stored therein?
(SECNAVINST 5510.36, 10-12) _____
11. Is there an SF 700 affixed inside each command security container?
(SECNAVINST 5510.36, 10-12) _____
12. Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination? (SECNAVINST 5510.36, 10-12) _____
13. Has the command established procedure for command key and padlock accountability and control? (SECNAVINST 5510.36, 10-13) _____
14. Are command locks repaired only by authorized personnel who have been subject to a trustworthiness determination or who are continuously escorted?
(SECNAVINST 5510.36, 10-15) _____

15. Are command security containers, previously placed out of service, marked as such on the outside and the "Test Certification Label" removed on the inside?
(SECNAVINST 5510.36, 10-15) ___ ___ ___
16. Are command security containers, with visible repair results, marked as such with a label posted inside the container stating the details of the repairs?
(SECNAVINST 5510.36, 10-15) ___ ___ ___
17. Are all commercial IDSS used on command security containers, vaults, modular vaults, and secure rooms approved by the CNO (N09N3)?
(SECNAVINST 5510.36, 10-16) ___ ___ ___
18. Is command classified information destroyed when no longer required?
(SECNAVINST 5510.36, 10-17) ___ ___ ___
19. Do all command shredders, pulverizers, and disintegrators meet the minimum requirements?
(SECNAVINST 5510.36, 10-18) ___ ___ ___
20. Has the command established effective procedures for the destruction of classified information? (SECNAVINST 5510.36, 10-19) ___ ___ ___
21. When filled, are command burn bags sealed and safeguarded per the highest overall classification level of their contents?
(SECNAVINST 5510.36, 10-19) ___ ___ ___
22. Is controlled unclassified information destroyed per the governing instruction?
(SECNAV 5510.36, 10-20) ___ ___ ___

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

1. Since the last inspection, has the command had any incidents involving a loss or compromise of classified information?
(SECNAVINST 5510.36, 12-1) ___ ___ ___
2. If a possible loss or compromise occurred, was a PI conducted? (SECNAVINST 5510.36, 12-4) ___ ___ ___
3. If a significant command weakness is identified, or a confirmed loss or compromise occurred, was a JAGMAN investigation conducted? (SECNAVINST 5510.36, 12-9) ___ ___ ___
4. When a loss or compromise of classified information or equipment has occurred, is appropriate investigative and remedial action(s) taken to ensure further loss or compromise does not recur?
(SECNAVINST 5510.36, 12-14) ___ ___ ___
5. Is appropriate and prompt corrective action taken whenever a knowing, willful, or

negligent compromise or repeated administrative disregard of security regulations occurs? (SECNAVINST 5510.36, 12-14) _____

6. Are procedures established for review of investigations by seniors? (SECNAVINST 5510.36, 12-14) _____

7. Are security reviews conducted on information subjected to loss or compromise? (SECNAVINST 5510.36, 12-15) _____

8. Is receipt of improperly transmitted information reported to the sender? (SECNAVINST 5510.36, 12-19) _____

SUPPLEMENTAL QUESTIONS

1. Is the command in possession of the following classified information references:

- a. WGO P5510.5 _____
- b. SECNAVINST 5510.34A _____
- c. OPNAVINST 5530.14B _____

2. Is the CMCC/scp custodian designated in writing? _____

3. Has the Command Security Manager developed SCP security procedures? (WGO P5510.5) _____

4. Has or does the emergency destruction plan: (SECNAVINST 5510.36, 2B-2)

- a. Give the exact location of classified material to be destroyed? _____
- b. Been tested at least every two years? _____
- c. Include priorities for destruction? _____
- d. Contain billet designations of personnel responsible for destruction? _____
- e. Have a predetermined destruction site and a particular piece of destruction equipment to be used? _____
- f. Clearly delineate the order of priority for use of the site or equipment? _____
- g. Authorized a senior individual in space containing classified material to deviate from established plans when circumstances warrant? _____
- h. Are records kept on file of emergency destruction tests for a period of 2 years? _____

5. Does the CMCC have an inspection and evaluation program for the secondary control point and/or sub-secondary control point to determine the effectiveness of information security program/procedures implementation? (WgO 5002.10) _____

a. Does the CMCC use prepared inspection Guidelines/Checklist? _____

- b. Are previous inspection reports on file? _____
- c. Have discrepancies been corrected? _____

- 6. Are there written procedures for accounting and controlling classified material (i.e. detailed turnover/desktop procedures order?) (WgO P5510.5) _____

- 7. Are administrative procedures established for controlling Secret material? (WgO P5510.5, 5001.2) _____

- 8. Are administrative procedures established for controlling confidential material? (WgO P5510.5, 5001.1) _____

- 9. Does the accounting system have the minimum required fields: (WgO P5510.5, 5001.3d) _____
 - a. Initial control number and/or originator (indicates wing/group/squadron/unit/organization) _____
 - b. Group/squadron CMCC control number? _____
 - c. Registered mail number? _____
 - d. Date of the document? _____
 - e. Copy number? _____
 - f. Date received? _____
 - g. Unclassified title? _____
 - h. Downgrading instructions? _____

- 10. Are restricted area warning signs posted at all normal points of ingress or egress? (SECNAVINST 5530.14, 3-8) _____

- 11. When language other than English is prevalent, are restricted area warning signs posted in English and the local language? (SECNAVINST 5530.14, 3-8) _____

- 12. Are classified document receipt records, inventory records, and control logs retained for two years as required by SECNAVINST P5212, Part II, PAR 5511? (WgO P5510.5, 5001.2C) _____

- 13. Are destruction records maintained for a period of 2 years for Secret material or 5 years for Top Secret material? (WgO P5510.5, 5001.2C & 5001.3C) _____

- 14. Has the SCP taken necessary security measures to ensure the protection of classification processed by ADP equipment? (WgO P5510.5, PAR 6002) _____

- 15. Is removable information media storage and devices, used with automatic data (ADP) systems and typewriters or word processing systems labeled using color-coded labels standard forms 706, 707, 708, 709, 710, 711? (WgO 5510.5, PAR 6003) _____

16. Are names, home addresses, and telephone numbers of personnel to be notified conspicuously posted on the safe in case of emergency or the safe being found opened? (WgO P5510.5)
17. Are classified messages over 90 days old controlled? (WgO P5510.5)
18. Has SCP custodian conducted a semi-annual classified material inventory/review during June/December? (WGO P5510.5D, PAR 4001.6B)
19. Were inventories/reviews forwarded to their respective chain of command? (WGO P5510.5D, PAR 4001.6B)
20. Are all classified 3.5 diskettes accounted for? WGO P5510.5D, PAR 8004.2)
21. Are classified diskettes placed in an appropriate folder with a diskette inventory sheet and a CMCC control card/number? (WGO P5510.5D, PAR 8004.3)
22. Are there any systems that process classified material connected to the local area network(LAN)? (WGO P5510.1, PAR 8008)

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____