U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 2nd ST SW
Washington, DC 20593-0001
Staff Symbol: G-CFI
Phone: (202)267-1990

COMDTNOTE 5510
17 JAN 2001
CANCELLED: 17 JAN 2002

COMMANDANT NOTICE 5510

Subj: CH-1 TO CLASSIFIED INFORMATION MANAGEMENT PROGRAM, COMDTINST M5510.23

1. PURPOSE. This Notice publishes changes to the Classified Information Management Program, COMDTINST M5510.23.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, Chief Counsel and special staff offices at Headquarters shall ensure compliance with the provisions of this Notice.

3. SUMMARY OF CHANGES. This change provides clarification to assist with implementation of the program, along with minor changes to previously published policy.

4. PROCEDURES. Remove and insert the following pages:

Remove	Insert
Pages i thru vii	Pages i thru viii CH-1
Pages 1-1 thru 1-7	Pages 1-1 thru 1-9 CH-1
Pages 2-1 thru 2-8	Pages 2-1 thru 2-8 CH-1
Pages 3-3, 3-4 and 3-9	Pages 3-3, 3-4 and 3-9 CH-1
Pages 4-1 thru 4-14	Pages 4-1 thru 4-14 CH-1
Pages 6-1 thru 6-10	Pages 6-1 thru 6-10 CH-1
Pages 8-5 thru 8-8, 8-11 and 8-12	Pages 8-5 thru 8-8, 8-11 and 8-12 CH-1
Pages 11-1, 11-2, 11-5, 11-6	Pages 11-1, 11-2, 11-5 , 11-6 CH-1
Pages 12-5, 12-6 and 12-11	Pages 12-5, 12-6 and 12-11 CH-1
Pages 13-1 and 13-2	Pages 13-1 and 13-2 CH-1
Pages 14-11, 14-12, 14-15, 14-16, 14-25 and 14-26	Pages 14-11, 14-12, 14-15, 14-16, 14-25 and 14-26 CH-1
Encl (1) all	Encl (1) Pages 1 thru 6 CH-1

ROBERT S. HOROWITZ
Acting Director of Finance and Procurement

DISTRIBUTION – SDL No.139

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	3	2	3		2	2	1	2	1	1		1	2	1	1	1	1		1		2					
B	1	8	10	2	12	5	3	5	3	3	2	3	3	10	3	2	2	40	2	1	2	1	3	2	1	1
C	3	2	1	3	2	1	1	1	2		2	1	2	5	2		3	1	2	1	1	1	1	1		
D	2	1	1	3	11	1	1	1	1	1	1	1	1			1	1	1	1	1	1	1	1			1
E		2	1				1	1		1	1	1	1	1	1				1							
F																			1							
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

TABLE OF CONTENTS

CHAPTER 1. - INTRODUCTION AND PROGRAM MANAGEMENT

A.	GENERAL	1-1
B.	INTRODUCTION	1-1
C.	PROGRAM MANAGEMENT	1-2
D.	RESPONSIBILITIES	1-4

CHAPTER 2. - CLASSIFICATION POLICY

A.	POLICY	2-1
B.	CLASSIFICATION PROHIBITIONS AND LIMITATIONS	2-1
C.	ORIGINAL CLASSIFICATION AUTHORITY	2-2
D.	DERIVATIVE CLASSIFICATION	2-2
E.	ACCOUNTABILITY OF DERIVATIVE CLASSIFIERS	2-4
F.	CLASSIFICATION LEVELS	2-4
G.	CLASSIFICATION GUIDES	2-4
H.	CLASSIFICATION CHALLENGES	2-5
I.	CLASSIFYING EQUIPMENT	2-5
J.	TENTATIVE CLASSIFICATION	2-6
K.	FOREIGN GOVERNMENT INFORMATION	2-6
	EXHIBIT 2-1 EQUIVALENT FOREIGN SECURITY CLASSIFICATIONS	2-9

CHAPTER 3. – MARKING

A.	INTRODUCTION	3-1
B.	MARKING DERIVATIVELY CLASSIFIED DOCUMENTS	3-1
C.	DERIVATIVELY CLASSIFYING FROM A SOURCE DOCUMENT	3-1
D.	DERIVATIVELY CLASSIFYING FROM MULTIPLE SOURCES	3-3
E.	MARKING INFORMATION TRANSMITTED ELECTRONICALLY	3-4
F.	DERIVATIVELY CLASSIFYING FROM A CLASSIFICATION GUIDE	3-5
G.	CLASSIFICATION EXTENSIONS	3-6
H.	FOREIGN GOVERNMENT INFORMATION	3-6
I.	RESTRICTED DATA	3-6
J.	FORMERLY RESTRICTED DATA	3-7
K.	LETTERS OF TRANSMITTAL	3-7

L. CLASSIFICATION MARKINGS ON DIFFERENT TYPES OF MATERIAL 3-8
M. INTELLIGENCE INFORMATION 3-9

CHAPTER 4. – SAFEGUARDING

A. BASIC POLICY 4-1
B. DEFINITIONS 4-1
C. STORAGE REQUIREMENTS 4-2
D. SPECIALIZED SECURITY CONTAINERS 4-3
E. EXCEPTION FROM STORAGE REQUIREMENTS 4-3
F. INSPECTION OF SECURITY CONTAINERS 4-3
G. COMBINATIONS 4-4
H. REPAIR OF SECURITY CONTAINERS 4-5
I. CONTAINER PRECAUTIONS 4-6
J. GENERAL SECURITY PRECAUTIONS 4-6
K. EMERGENCY PLANNING 4-7
L. RESTRICTED AREAS 4-9
M. UNAUTHORIZED ACCESS 4-10
N. CLASSIFIED SPACES 4-10

CHAPTER 5. – CLASSIFIED VISITS AND MEETINGS

A. VISITS INVOLVING ACCESS TO CLASSIFIED INFORMATION 5-1
B. CLASSIFIED MEETINGS, CONFERENCES & TRAINING SESSIONS 5-9

CHAPTER 6. – ACCESS, ACCOUNTABILITY AND CONTROL SYSTEM

A. ACCESS 6-1
B. ACCOUNTABILITY AND CONTROL SYSTEMS 6-1
C. SECURITY CONTROL POINT 6-2
D. DOCUMENT CONTROL STATION 6-2
E. ACCOUNTABILITY RECORDS 6-3
F. EXCEPTIONS FROM ACCOUNTABILITY 6-3
G. RECEIPT OF CLASSIFIED MATERIAL 6-5
H. RECORD OF DESTRUCTION 6-6
I. CHANGES IN ACCOUNTABILITY 6-6
J. TOP SECRET DISCLOSURE RECORDS 6-6
K. INVENTORY REQUIREMENTS 6-7

L. CHANGES AND CORRECTIONS 6-8
M. PAGE CHECKS 6-8
N. WORKING PAPERS 6-8
O. MAGNETIC/OPTICAL MEDIA 6-9
P. CLASSIFIED MATERIAL IS NOT PERSONAL PROPERTY 6-9
EXHIBIT 6-1, PUBLICATION CHANGE CHECK LIST 6-10

CHAPTER 7. – DISSEMINATION AND REPRODUCTION

A. DISSEMINATION OF CLASSIFIED MATERIAL 7-1
B. DISCLOSURE OUTSIDE THE EXECUTIVE BRANCH OF GOVERNMENT 7-2
C. REPRODUCTION OF CLASSIFIED INFORMATION 7-3
D. PRINTING AND PHOTOGRAPHIC PROCESS 7-5
E. CONTROL OF PHOTOGRAPHIC EQUIPMENT 7-5

CHAPTER 8. – TRANSMISSION OF CLASSIFIED MATERIAL

A. POLICY 8-1
B. TOP SECRET TRANSMISSION 8-1
C. SECRET TRANSMISSION 8-1
D. CONFIDENTIAL TRANSMISSION 8-3
E. TRANSMISSION TO FOREIGN GOVERNMENTS 8-4
F. CONSIGNOR-CONSIGNEE RESPONSIBILITY FOR SHIPMENT OF BULKY MATERIAL 8-5
G. TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL 8-6
H. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION 8-6
I. RECEIPT SYSTEM 8-8
J. HANDCARRYING CLASSIFIED MATERIAL 8-8

CHAPTER 9. – FOREIGN DISCLOSURE

A. DISCLOSURE TO FOREIGN GOVERNMENTS, FOREIGN NATIONALS AND INTERNATIONAL ORGANIZATIONS 9-1
B. DELEGATION OF DISCLOSURE

AUTHORITY 9-1

CHAPTER 10. - DECLASSIFICATION AND DOWNGRADING

A. GENERAL 10-1
B. DECLASSIFICATION SYSTEMS 10-1
C. CLASSIFIED INFORMATION TRANSFERRED TO THE COAST GUARD 10-3
D. DECLASSIFICATION DATABASE 10-3
E. DOWNGRADING 10-4
F. UPGRADING 10-4
G. FREEDOM OF INFORMATION ACT (FOIA) AND PRIVACY ACT REQUESTS 10-4

CHAPTER 11. – DESTRUCTION

A. GENERAL 11-1
B. APPROVED DESTRUCTION METHODS 11-1
C. DESTRUCTION PROCEDURES 11-3
D. CLASSIFIED WASTE 11-3
E. EMERGENCY DESTRUCTION 11-4
F. PRIORITY FOR EMERGENCY DESTRUCTION 11-5
G. REPORTING EMERGENCY DESTRUCTION 11-6

CHAPTER 12. – COMPROMISES, ADMINISTRATIVE DISCREPANCIES, WAIVERS & EXCEPTIONS

A. INTRODUCTION 12-1
B. COMPROMISE 12-1
C. ADMINISTRATIVE DISCREPANCY 12-1
D. INITIAL REPORTING AND RESPONSIBILITIES 12-1
E. SECURITY INVESTIGATIONS 12-6
F. ADMINISTRATIVE INVESTIGATIONS 12-6
G. INVESTIGATION ASSISTANCE 12-7
H. INCIDENTS INVOLVING SPECIAL TYPES OF INFORMATION 12-7
I. COMPROMISE THROUGH PUBLIC MEDIA 12-7
J. DEBRIEFINGS IN CASE OF UNAUTHORIZED ACCESS 12-8
K. WAIVERS AND EXCEPTIONS 12-8

EXHIBIT 12-1 EXAMPLE OF AN INCIDENT INVOLVING CLASSIFIED MATERIAL REPORT 12-11

CHAPTER 13. – SPECIAL CATEGORIES OF INFORMATION

A. GENERAL 13-1
B. SPECIAL ACCESS PROGRAM (SAP) 13-1
C. SENSITIVE COMPARTMENTED INFORMATION (SCI) 13-1
D. RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATE (FRD) 13-1

CHAPTER 14. – OPERATIONS SECURITY (OPSEC)

A. INTRODUCTION 14-1
B. APPLICATION 14-1
C. RESPONSIBILITIES 14-3
D. OPSEC SURVEYS 14-3
EXHIBIT 14-1 INDICATOR TABLES 14-4
EXHIBIT 14-2 COUNTERMEASURE TABLES 14-22

ENCLOSURES

(1) INFORMATION SECURITY EVALUATION CHECKLIST
(2) SAMPLE INFORMATION SECURITY PLAN

PUBLICATION CHANGE RECOMMENDATION (PCR)

USE THIS PAGE TO MAKE RECOMMENDATIONS FOR THIS PUBLICATION

1. Identify each section you comment on by page number, paragraph, section, or figure.
2. Clearly identify the problem with the publication.
3. State your suggested solution to the problem. Include suggested wording or drawings.
4. Mail to : **Commandant (G-CFI)**
   U.S. Coast Guard **Via: Cognizant Security Manager**
   2100 Second Street, SW
   Washington, D.C. 20593-0001
5. G-CFI will assign a PCR number to the recommendation and will reply to the originator by mail.

CLASSIFIED INFORMATION MANAGEMENT PROGRAM, COMDTINST M5510.23

PAGE	PARA.	PROBLEM OR REASON FOR CHANGE:

RECOMMENDED CHANGE: (BE SPECIFIC ON HOW YOU THINK IT SHOULD BE WORDED OR APPEAR)

(CONTINUE YOUR REMARKS ON 8.5"x 11 PAPER IF ADDITIONAL SPACE IS NEEDED)

ORIGINATING UNIT ADDRESS:
(INCLUDE UNIT POC , PHONE NO. & EMAIL)

SECURITY MANAGER ENDORSEMENT	
[ ] **CONCUR**	[ ] **DO NOT CONCUR**

REMARKS:

DATE:	TYPED NAME:	SIGNATURE:

CGHQ PCR NO.: CIMP-	ACTION:	DATE:

PLEASE CLOSE WITH TAPE – DO NOT STAPLE – THANK YOU

(FOLD HERE)

U.S. Department
Of Transportation
United States
Coast Guard
2100 Second St. SW
Washington, D.C. 20593-0001

Commandant (G-CFI)
U.S. Coast Guard
2100 Second Street, SW
Washington, D.C. 20593-0001

(FOLD HERE)

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE ENTERED	ENTERED BY (Printed name and signature)

CHAPTER ONE - INTRODUCTION TO AND MANAGEMENT OF THE SECURITY PROGRAM AND CLASSIFIED INFORMATION

A. GENERAL.

1. This chapter establishes policy and guidance for managing the classified information program at individual units. The Commanding Officer is ultimately responsible for the security of classified information at his or her command. In addition, every individual in the Coast Guard is directly responsible for supporting the Coast Guard Classified Information Management Program.

2. For the purpose of this manual, Commanding Officer includes Commanders and Officer-in-Charge. Cognizant Security Managers (SECMGR) include Area and District SECMGRs. Major units include Headquarters, Groups, Air Stations, Marine Safety Offices (MSOs), Area and District staffs, Integrated Support Commands (ISCs), Electronic Support Units (ESUs), Communications Stations and all Cutters 180' and larger.

3. Recommendations for changes to this manual are encouraged and shall be forwarded to Commandant (G-CFI), the Classified Information Management Program Manager, via the cognizant Area or District SECMGR. Comments or proposed changes shall be specific and include justification or documentation necessary to ensure proper evaluation.

B. INTRODUCTION.

1. Executive Order (EO) 12958 (60 Fed. Reg. 19,825 (1995)), prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

2. National security information is any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. Information shall be classified only when necessary in the interest of national security.

3. Official information does not need to be classified Confidential, Secret or Top Secret to be protected. The guidelines set forth in this manual and related instructions shall be closely followed to insure that all original and derivative classification decisions made within the Coast Guard are consistent with national policy. Unclassified information which has been

properly marked "For Official Use Only" (FOUO) may require protection under the Coast Guard Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3 (series).

4. The Coast Guard Classified Information Management Program is designed to promote proper and effective classification, protection and downgrading of national security information. It also promotes the declassification of information no longer requiring such protection.

5. The security of the United States in general, and of Coast Guard operations in particular, depends in part upon the success attained in the safeguarding of national security information. Sound direction and program implementation is critical to the attainment of proper handling and safeguarding objectives.

6. All Coast Guard personnel are personally and individually responsible for providing proper protection to classified information under their custody and control.

7. This manual provides Coast Guard guidance for the Classified Information Management Program.

C. PROGRAM MANAGEMENT.

1. Executive Office Of the President.

   a. The National Security Council (NSC) may review all matters with respect to the implementation of EO 12958 and shall provide overall policy direction for classified national security information.

   b. The Director of the Information Security Oversight Office (ISOO), a component of the National Archives and Records Administration (NARA), is responsible for the following functions:

      (1) Development and implementation of directives and instructions.

      (2) Maintaining liaison with agency counterparts to conduct on sight inspections and special document reviews to monitor agency compliance.

      (3) Developing and disseminating security education materials for Government and industry.

      (4) Monitoring security education and training programs.

(5) Receiving and taking action on complaints, appeals, and suggestions.

(6) Collecting and analyzing relevant statistical data and report them annually, along with other information, to the President.

(7) Serving as spokesperson to the Congress, the media, special interest groups, professional organizations, and the public.

(8) Conducting special studies on identified or potential problem areas and develop remedial approaches for program improvement.

(9) Providing program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).

c. The Director of ISOO is authorized to request information or material concerning the Department of Transportation (DOT), including the Coast Guard, needed by the ISOO in carrying out its functions.

2. Department of Transportation. The Assistant Secretary for Administration, DOT, has been designated as the senior staff officer to the Secretary of Transportation with assigned responsibilities to assure effective compliance with EO 12958. That office has been authorized to issue DOT-wide policy to implement the EO and, in this regard, has issued DOT Order 1640.4 (series), Classified Information Management. The Director, Office of Security and Administration, Office of the Secretary of Transportation (OST), has responsibilities to evaluate the application of and adherence to the security policies prescribed by DOT order 1640.4 (series).

3. Commandant, U. S. Coast Guard. Commandant (G-CFI) is the program manager for the Coast Guard Classified Information Management Program and is responsible for:

a. Monitoring and overseeing the Coast Guard Classified Information Management Program.

b. Managing and evaluating the Coast Guard Classified Information Management Program

c. Developing and implementing plans, policies, procedures and standards, and providing programmatic guidance and direction for the Coast Guard Classified Information Management Program.

D. RESPONSIBILITIES.

1. Commandant, U. S. Coast Guard. Commandant (G-CFI) manages and oversees the overall Coast Guard Security Program. G-CFI serves as the Director of Coast Guard Security, Security Advisor to the Commandant and as representative at the national and international and congressional levels for internal security and counterintelligence related matters. As such, G-CFI is responsible for:

a. Managing, overseeing, developing, reviewing, evaluating and promulgating plans, policies, and procedures for the following elements of the overall USCG Security Program: Physical Security; Loss Prevention; Information Security; Personnel Security and Suitability for Service; Industrial Security; Security Countermeasures; Technical Security; Force Protection, which includes Antiterrorism/Force Protection and Counterterrorism; Critical Infrastructure Protection; Security Awareness and Education; Operation Security; Counterintelligence; Police Services; Acquisition Security; and other internal security elements, programs and functions.

b. . Developing, managing, overseeing and directing the Coast Guard Classification Management Program and serving as the USCG final authority for classification and declassification matters, as they pertain to classified national security information in accordance with applicable executive orders, reporting directly to the Coast Guard Original Classification Authorities, the Commandant and the Assistant Commandant for Operations.

c. Monitoring, reviewing and evaluating all aspects of Information Systems Security and Communications Security for consistency with the overall USCG Security Program, and providing programmatic guidance to the designated program managers for each of these Internal Security Program elements.

d. Reviewing and evaluating regularly the effectiveness of policy and program implementation by support and operating programs and field commands. Managing the research, development, and preparation of annual reports to Congress, regarding the cost of protecting classified National Security related information, personnel security clearances, and other related requirements and requests; and developing and promulgating responses to

congressional inquiries.

e. Developing the criteria for and managing the recruitment, evaluation, selection and certification of USCG Area and District Security Managers and other security management personnel, and providing technical direction and guidance.

f. Managing the USCG Loss Prevention Program, and evaluating all incidents within the Coast Guard involving the loss or compromise of classified information or material, and the loss or theft of government property, assets, weapons, money, material and sensitive and technical information.

g. Serving as the USCG Final Reviewing Authority for all security and counterintelligence related Administrative Investigations or Inquiries.

NOTE: *The requirements in this manual do not apply to Communications Security (COMSEC) Facilities, which are covered by Communications Security Material System Policy and Procedures Manual (CMS-1(series)/CMS-21(series)) or Sensitive Compartment Information Facilities (SCIF) which is covered by Director of Central Intelligence Directive 1/21 (DCID 1/21).*

2. Security Managers. The Security Manager works under the direction of the area/district Chief of Staff. The Security Manager is responsible for:

a. Monitoring and overseeing the implementation of the Coast Guard Classified Information Management Program for all units within their Area of Responsibility (AOR). Maintain liaison with the cognizant command security personnel and provide assistance as appropriate.

b. Conducting a biennial evaluation of Area, MLC and major district units (District Security Managers will evaluate Headquarters units geographically located within their district), using the evaluation check sheet provided as enclosure (1) to this manual. A written report of evaluation will be provided to the unit, and a copy of the report provided to Commandant (G-CFI).

c. Serving as the security advisor to the Area or District Commander.

d. Ensuring that an active, comprehensive security awareness, education and training program for the protection of national

security information, assets and personnel is in place throughout their AOR, and exercise oversight of this program.

e. Developing and promulgating additional guidance and procedures for the protection of national security information, Coast Guard assets and personnel throughout their AOR.

f. Reviewing, evaluating, investigating, and following up on cases where national security information is subjected to possible compromise. Ensure proper reports are completed in accordance with chapter 12 of this Manual.

g. Granting waivers and endorsing exceptions from security requirements contained within this Manual.

3. Command Security Officer (CSO). The CSO works under the direction of the Commanding Officer, who is ultimately responsible for all national security information at his/her unit. The CSO shall be a commissioned officer, chief warrant officer, senior petty officer (E-7 through E-9) or civilian employee (GS-9 or above). The Commanding Officer shall designate the CSO in writing with a copy to the cognizant Security Manager. The CSO is responsible for:

a. Becoming familiar with the requirements of all security related Commandant, Area and District instructions, and is responsible for all subordinate units under their cognizance.

b. Serving as the unit commander's security advisor and point of contact for security and counterintelligence related matters.

c. Promulgating and implementing security programs, policies, plans and procedures, as required by all applicable security instructions, and assist subordinate units with compliance.

d. Conducting an annual self evaluation of parent and subordinate commands, using the evaluation check sheet provided as enclosure (1) to this manual, and forwarding a copy of the written evaluation to the cognizant security manager.

e. Ensuring that all persons who handle classified information are appropriately cleared and have received the proper briefings.

f. Promulgating and implementing additional security measures for the protection of national security information, Coast Guard assets and personnel throughout their area of responsibility.

g. Ensuring that an effective classified material control system is in place.

h. Serving as the point of contact for matters pertaining to classified visit requests to the unit.

i. Maintaining liaison with the unit public affairs officer to ensure that proposed public releases, which could possibly contain classified information, are reviewed prior to release.

j. Ensuring subordinate units are evaluated and trained annually in all security programs, plans, policies, procedures and security force operations, as contained in internal security related instructions.

k. Providing to the cognizant security manager the number of derivative classifications made by the unit (including subordinates) each fiscal year.

l. Providing to the cognizant security manager the total costs incurred by the unit to safeguard classified material each fiscal year.

4. Classified Material Control Officers (CMCO). The CMCO shall be designated in writing and copies forwarded to the CSO and Security Manager. The CMCO works under the direction of the CSO and is responsible for:

a. Maintaining accountability records for the security control point (SCP).

b. Ensuring the proper operation of the classified material control system (CMC).

c. Identifying classified material to be returned to the originating unit when required.

d. Verifying the clearance status of initial recipients on incoming classified material.

e. Routing downgrading and/or declassification notices to the holders of the classified material involved.

f. Inspecting all classified material received by the unit for tampering or damage.

g. Matching the actual contents of an incoming package of classified material with the enclosed receipt.

h. Destroying or arrange for the destruction of classified material within the CMC system as appropriate.

i. Ensuring that the appropriate method of transmission (except telecommunications) is selected for all outgoing classified material and that it is properly prepared for transmission.

j. Maintaining a program for the reduction of classified holdings by continually reviewing applicable instruction, notices and general messages.

k. Determining the continued need for retention of classified material with the custodian or cognizant official.

l. Ensuring changes to classified publications are entered correctly and in a timely manner.

m. Ensuring that receipts are obtained for classified material sent from the unit.

n. Signing and returning to the sender all receipts enclosed in classified transmittals.

o. Ensuring inventories of classified material are conducted as required.

p. Maintaining records pertaining to the identity and security clearance level of each Document Control Station Officer (DCSO) if applicable.

q. Maintaining a system of accountability which will record the source, downgrading, movement from one office to another, current custodian, destruction or other disposition of all top secret material for which responsible.

r. Keeping dissemination of top secret information to the absolute minimum necessary for proper planning or action. There will be no
"standard routing" for top secret material within a unit.

s. Ensuring that a system is established to transmit top secret material within the unit by direct personal contact. The CMCO does not have to deliver the material personally but the material has to be

delivered directly to the person who is to assume responsibility for it.

t. Maintaining a continuous chain of signed receipts and disclosure record (CG-4764A) for all top secret material. Person-to-person contact is required for the receipt process.

u. Ensuring that a physical inventory of top secret material is conducted at least once every six months.

v. Maintaining a current roster of persons within the unit who are authorized access to top secret information. The CMCO should know who in the unit requires top secret access and be able to assist the CSO in determinations of access to be granted at the unit.

w. Ensuring that all top secret material is accounted for and properly transferred when custodians are relieved of their duties. This requirement applies to the sub-custodians of the unit as well as the CMCO.

5. Document Control Station Officer (DCSO). The DCSO works under the direction of the CMCO and shall be designated in writing. The DCSO is responsible for:

a. Receiving and transmitting through the security control point, all classified material flowing in and out of the element which is being serviced.

b. Maintaining a record of all accountable material and shall further identify the custodian of the material.

c. Ensuring that only those persons who maintain appropriate security clearances and have a valid need-to-know have access to such material.

CHAPTER TWO - CLASSIFICATION POLICY

A. POLICY.

1. Except for information subject to the Atomic Energy Act of 1954 (as amended), EO 12958 and this Manual provide the only basis for classification within the Coast Guard.

2. EO 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open government.

3. Information shall be classified only when necessary in the **interest of national security**, and shall be declassified as soon as is consistent with the requirements of national security.

4. Information shall not be reclassified after it has been declassified and officially released to the public by proper authority.

B. CLASSIFICATION PROHIBITIONS AND LIMITATIONS.

1. In no case shall information be classified in order to:

   a. Conceal violations of law, inefficiency, or administrative error.

   b. Prevent embarrassment to a person, organization, or agency.

   c. Restrain competition.

   d. Prevent or delay the release of information that does not require protection in the interest of national security.

C. ORIGINAL CLASSIFICATION AUTHORITY.

1. 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.

2. Coast Guard original classification authorities have been specifically delegated by the Secretary of Transportation, and have received training in the exercise of this authority. This authority is personal and is vested only in the individual occupying the position. The authority may not be exercised "by direction" of a designated official. The formal appointment or assignment of an individual to one of the positions identified below or assignment of an individual to one of the identified positions designated in writing to act in their absence conveys the authority to originally classify information as secret and below.

3. The Commandant (G-C) and the Assistant Commandant for Operations (G-O) have been delegated as original classification authorities within the Coast Guard and have the authority to originally classify information as secret and below.

4. Information not already classified by an original classification authority may not be marked as classified. Cases of original classification by other than an original classification authority will be reported to Commandant (G-CFI) in accordance with chapter 12 of this manual.

5. Due to the limited number of Coast Guard personnel delegated to originally classify information, original classification instructions will be published in COMDTINST M5510.1(series) with limited distribution.

D. DERIVATIVE CLASSIFICATION.

1. Process. Derivative classification is the process of determining whether information that is to be included in a document or material has been classified and, if it has, ensuring that it is identified as classified information by marking or similar means. Information is derivatively classified whenever it is extracted, paraphrased, restated, or generated in a new form. Application of classification markings to a document or other material is as directed by a security classification guide or other source material classified by an original classification authority. Simply photocopying or otherwise mechanically reproducing classified material is not derivative classification.

2. Authority and Responsibility. Within the Coast Guard, all cleared personnel who generate or create material that should be derivatively classified are responsible for ensuring that the derivative classification is accomplished in accordance with chapter 3. Persons conducting the derivative classification require no specific delegation of authority. Coast Guard officials who sign or approve derivatively classified documents have principal responsibility for the quality of the derivative classification they sign or approve.

3. Policy. All persons performing derivative classification shall:

   a. Respect original classification decisions.

   b. Apply markings or other means of identification to derivatively classified material as required by chapter 3 of this manual.

   c. Use only authorized sources of instructions about the classification of the information in question. Authorized sources of instruction about classification are security classification guides, other forms of classification guidance, and markings on material from which the information is extracted. The use of only memory or "general rules" about the broad classes of information is prohibited.

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

   e. Remember, other persons may use your derivative document as a source for other derivative classification decisions. An error in derivative classification could be repeated numerous times before notification is made, resulting in several documents incorrectly classified as a result of a mistake.

4. Procedures.

   a. Derivative classifiers must carefully analyze the material they are classifying to determine what information it contains or reveals and ensure that it meets the requirements of the classification guidance or the markings on the source document.

   b. When material is derivatively classified based on "multiple sources" (more than one security classification guide, classified source document, or combination thereof), the derivative classifier must compile a list of the sources used. A copy of this list must be included in or attached to the file or record copy of the document

and retained at the command until the sources used are declassified.

E. <u>ACCOUNTABILITY OF DERIVATIVE CLASSIFIERS</u>. Each derivative classifier is accountable for the legitimacy of the classifications he/she assigns. Before approving and signing classified documents, officials with command signature authority shall ensure that classification markings are in accordance with chapter 3 of this manual, and that the derivative classification is based on a source document or classification guide issued by an original classification authority. Commands shall track and provide to the security manager the quantity of derivative classification decisions made for each fiscal year.

F. <u>CLASSIFICATION LEVELS</u>.

1. Information which requires protection against unauthorized disclosure in the interest of national security shall be classified Top Secret, Secret, or Confidential. No other terms shall be used to identify classified information. Classification levels are assigned to determine the level of protection and the damage an unauthorized disclosure could cause. The three classification levels are:

   a. Top Secret. Is information requiring the highest degree of protection. The unauthorized disclosure of top secret information could reasonably be expected to cause exceptionally grave damage to the national security.

   b. Secret. Is information requiring a substantial degree of protection. The unauthorized disclosure of secret information could reasonably be expected to cause serious damage to the national security.

   c. Confidential. Is information requiring protection. The unauthorized disclosure of confidential information could reasonably be expected to cause damage to national security.

G. <u>CLASSIFICATION GUIDES</u>.

1. A classification guide is an instruction which prescribes the appropriate classification designation and declassification guidance, for categories of related information, promulgated by the program manager responsible for that information, and personally approved in writing by an original classification authority. Classification guides are intended to facilitate the proper and uniform derivative classification of information. A classification guide must be prepared for each system, plan, program or project involving classified information and promulgated as soon as

practicable prior to initial implementation of the program. All classification guides shall be coordinated with Commandant (G-CFI).

2. Classification guides shall be unclassified if at all possible and as a minimum include the following:

   a. Identity of the information to be protected, using whatever terms are necessary to ensure that the protected information can be easily identified.

   b. State the level of classification that applies to the information, either secret or confidential. No one within the Coast Guard may originally classify information at the Top Secret level.

   c. Specify the duration of each classification, in terms of a period of time or the occurrence of an event.

3. All Coast Guard classification guides shall be issued in the form of a Commandant Instruction and distributed as appropriate. Classification guides from other agencies may be requested as needed from the appropriate agency.

H. CLASSIFICATION CHALLENGES.

1. Holders of information who believe it is inappropriately classified, or inappropriately unclassified, are expected to challenge the classification status of the information. Coast Guard members are encouraged to informally question the classification status of information. If informal questioning does not resolve the challenge, a written challenge should be submitted.

2. Requests for classification challenges should be submitted to Commandant (G-CFI) who will:

   a. Conduct a security review, to include consultation with the originator of the document and the original classification authority (if classified).

   b. Provide written response to the challenger.

I. CLASSIFYING EQUIPMENT.

1. Items of equipment or other physical objects shall be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or by their operation, test, application or use. The overall classification assigned to end items of

equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

2. If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

J. <u>TENTATIVE CLASSIFICATION</u>. If information is originated by an individual who does not have original classification authority and that individual believes the information should be classified, he/she shall:

1. Safeguard the information in the manner prescribed for the level of classification believed to be appropriate.

2. Mark the information with the believed classification level, with a notation in the first line of the text stating "THIS INFORMATION HAS BEEN TENTATIVELY CLASSIFIED PENDING AN ORIGINAL CLASSIFICATION DECISION".

3. Forward the information, via the cognizant security manager, to Commandant (G-CFI), with a cover memo stating that the information is tentatively marked to protect it in transit. Justification for the classification shall also be included in the memo. A determination as to whether to classify the information shall be made by appropriate authority and the tentative classifier will be notified of the results.

4. If urgent operational needs require immediate communication of the information to any unit, it shall be safeguarded and marked as described above and transmitted by message. The written request for evaluation shall then be sent to Commandant (G-CFI) with a copy to the cognizant security manager. Include in the memo of transmittal all units who have received the information so they may be informed of the results of the determination of the original classification authority.

5. Upon a decision by the original classification authority, the tentative notation will be removed. If a classification is assigned, appropriate markings will apply.

K. <u>FOREIGN GOVERNMENT INFORMATION</u>. Foreign government information falls into one of the two categories:

1. Information provided to the U.S. by a foreign government or international organization of governments, such as the North Atlantic Treaty Organization (NATO), where the U.S. has undertaken an obligation, expressed or implied, to keep the information in confidence. The information is considered to have been provided in confidence if it is marked in a manner indicating it is to be treated in confidence or if the

circumstances of the delivery indicate that the information is to be kept in confidence.

2. Information requiring confidentiality, produced by the U. S. pursuant to a written joint arrangement with a foreign government or international organization of governments. A written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record of the joint arrangement.

3. Classification.

   a. Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a U. S. classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

   b. Foreign government information that was not classified by a foreign entity but was provided to the Coast Guard with the expressed or implied obligation that it be held in confidence shall be classified. The classification process outlined in this chapter does not apply to the classification of such foreign government information. Such foreign government information shall be afforded the protection given to information classified at the confidential level until an original classification authority can make a classification determination. At the time of classification, however, judicious consideration shall be given to the sensitivity of the subject matter and the impact of its unauthorized disclosure upon both the U. S. and the originating foreign government or organization of governments in order to determine the most appropriate level of classification. In weighing the need to protect foreign government information and confidential foreign sources against the possible public interest in disclosure, the need to protect such information shall be presumed to predominate. An original classification authority shall assign levels above Confidential.

4. Duration of Classification. Foreign government information shall be classified as long as necessary in the interest of national security.

5. Declassification. In considering the possibility of declassification of foreign government information, officials shall respect the intent of this manual to protect foreign government information and confidential foreign sources.

6. Mandatory Review. Requests for mandatory review for declassification of foreign government information shall be forwarded to Commandant (G-CFI).

7. Equivalent U.S. Classifications. Foreign classifications generally parallel U. S. classifications. A table of equivalent classifications is contained in exhibit 2-1.

8. Marking. Chapter 3 of this manual provides guidance on marking foreign government information. Detailed guidance for marking NATO material may be found in the NATO Security Manual, COMDTINST M5500.19 (series).

9. Protective Measures.

   a. NATO Classified Information. NATO Classified information shall be safeguarded in accordance with the provisions of the NATO security Manual, COMDTINST M5500.19(series).

   b. Other Foreign Government Information. Classified foreign government information other than NATO information shall be protected as is prescribed by this manual for U. S. classified information of a comparable classification

CHAPTER THREE - MARKING

A. <u>INTRODUCTION</u>. Executive Order 12958 requires that all classified national security information be marked to place recipients on alert about its sensitivity. This chapter provides a general guide on these marking requirements. It is intended for use by derivative classifiers as well as administrative personnel who may prepare the final product. Marking instructions for designated original classifiers are contained in COMDTINST M5510.1 (series). All security markings used in this chapter are for illustration purposes only.

B. <u>MARKING DERIVATIVELY CLASSIFIED DOCUMENTS</u>. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a classification guide issued by an original classification authority.

C. <u>DERIVATIVELY CLASSIFYING FROM A SOURCE DOCUMENT</u>.

1. When using a classified source document as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document.

2. Exhibit 3-1 is a properly marked source document and a properly marked derivative document. The derivative document contains information taken from paragraph two of the source document. The following will retrace the steps that are necessary to mark a document derived from a classified source.

   a. Portion Marking. The first paragraph of the derivative document incorporates information from the second paragraph of the source document, a paragraph marked "Secret". Therefore, portion mark the first paragraph of the derivative document with an "(S)". The derivative document contains no other classified information. Therefore, portion mark all other portions with a "(U)". Exhibit 3-2 illustrates.

SOURCE DOCUMENT

SECRET

5510
May 28, 1998

Subject: Funding Problems **(U)**

1. **(U)** This is paragraph 1 and it contains **unclassified** information. Therefore, this portion will be marked with the designation **"U"** in parentheses.

2. **(S)** This is paragraph 2 and it contains **Secret** information. Therefore, this portion will be marked with the designation "**S**" in parentheses.

3. **(C)**This is paragraph 3 and it contains **Confidential** information. Therefore, this portion will be marked with the designation "C" in parentheses.

J. J.Jones
By direction

Classified by: ADM J. M. LOY
COMMANDANT
Reason: 1.5(a) and (d)
Declassify on: December 31, 2006

SECRET

DERIVATIVE DOCUMENT

SECRET

5510
June 15, 1998

Subject: Recommendations for resolving Funding Problems **(U)**

1. **(S)** This is paragraph 1 and it contains **Secret** information **taken from paragraph 2 of the source document**. Therefore, this portion will be marked with the designation "**S**" in parentheses.

2. **(U)** This is paragraph 2 and contains **unclassified** information. Therefore, this portion will be marked with the designation "**U**" in parentheses.

3. **(U)** This is paragraph 3 and contains **unclassified** information. Therefore, this portion will be marked with the designation "**U**" in parentheses

R. ISOO
Acting

Derived From: **COMDT ltr 5510 dtd May 28, 1998**
Subj: Funding Problems

Declassify on: **December 31, 2006**

SECRET

EHXIBIT 3-1

DERIVATIVE DOCUMENT

SECRET

5510
June 15, 1998

Subject: Recommendations for resolving Funding Problems **(U)**

4. **(S)** This is paragraph 1 and it contains **Secret** information **taken from paragraph 2 of the source document**. Therefore, this portion will be marked with the designation "**S**" in parentheses.

5. **(U)** This is paragraph 2 and contains **unclassified** information. Therefore, this portion will be marked with the designation "**U**" in parentheses.

6. **(U)** This is paragraph 3 and contains **unclassified** information. Therefore, this portion will be marked with the designation "**U**" in parentheses

R. ISOO
Acting

Derived From: **COMDT ltr 5510 dtd May 28, 1998**
Subj: Funding Problems

Declassify on: **December 31, 2006**

SECRET

EHXIBIT 3-2

b. Overall Classification Markings. The highest classification level of any portion of this derivative document is "Secret". Therefore, conspicuously place an overall classification of "Secret" at the top and bottom of the derivative document as shown in exhibit 3-3. If the derivative document contains more than one page, place the overall marking at the top and bottom of the outside of the from cover, on the title page, on the first page, and on the outside of the back cover. Mark other internal pages either with the overall classification or with a marking indicating the highest classification level of information contained on that page.

DERIVATIVE DOCUMENT
SECRET

SECRET

EXHIBIT 3-3

c. Derived from line. Identify the source used as the basis for classification on the "Derived from" line of the derivative document, as shown in exhibit 3-4.

d. Declassify on line. Carry forward the duration of classification from the "Declassify on" line of the source document to the "Declassify on" line of the derivative document, as shown in exhibit 3-5. When the "Declassify on" line of the source document is marked "Originating Agency's Determination Required" or "OADR", mark the "Declassify on" line of the derivative document to indicate:

DERIVATIVE DOCUMENT
SECRET

Derived From: COMDT ltr 5510 dtd May 28, 1998
Subj: Funding Problems

SECRET

EXHIBIT 3-4

(1) The fact that the source document is marked with this instruction.

(2) The date of origin of the source document.

(3) This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under EO 12958.

DERIVATIVE DOCUMENT
SECRET

Declassify on: December 31, 2006

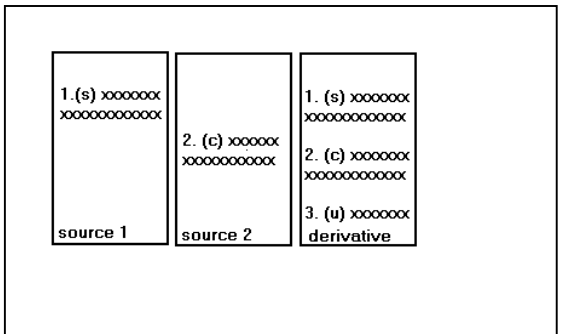
SECRET

EXHIBIT 3-5

NOTE: The declassification instruction "Originating Agency's Determination Required" or "OADR" would only be valid for a source document which has not yet been updated and was issued before October 14, 1995 (the effective date of EO 12958).

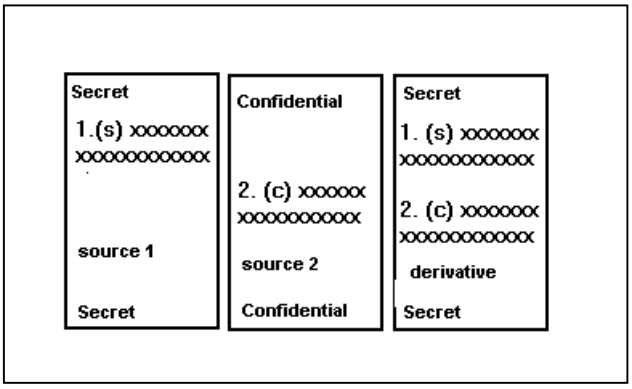
D. <u>DERIVATIVELY CLASSIFYING FROM MULTIPLE SOURCES</u>.

1. Portion Marking. When using more than one classified source document in creating a derivative document, portion mark the



classified information incorporated in the derivative document with the level indicated on the source documents. Portion mark all other portions "(U)". In exhibit 3-6, paragraph one of the derivative document incorporates "Secret" information from paragraph one of source 1 and paragraph two of the derivative document incorporates "Confidential" information from paragraph two of source 2. The remainder is unclassified.

2. Overall Classification Marking. onspicuously mark the derivative document at the top and bottom with the highest classification level of information found in any portion of the document. In the example shown, the overall classification is "Secret". If the derivative document contains more than one page, each page needs to be marked with an overall marking. See exhibit 3-7.



3. Derived From Line. Enter the standard notation "Multiple Sources" on the "Derived from" line of the derivative document to indicate that more than one classified source was used. See exhibit 3-8.

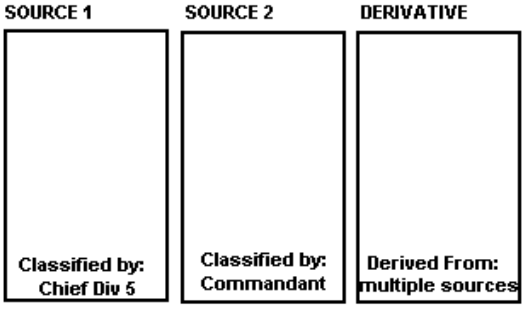


EXHIBIT 3-8

Maintain the identification of all classified sources with the file or record copy of the derivative document. If practicable, include the list with all copies of the derivative document. See exhibit 3-9.

Official File Copy

Derived From: Multiple Sources

Source 1: Memo of May 4, 2004
David Smith
Chief, Division 5
Source 2: Report of Oct 20, 1996
Adm Smith
Commandant

EXHIBIT 3-9

4. Source Document Marked "Multiple Sources". Deriving classified information from a source document that is itself marked "Multiple Sources" presents a special problem in identifying that document on the "derived from" line of the new document. Do not carry forward the notation "Multiple Sources" to the new document, because the document could not then be used to trace the actual sources of classification. Instead, specifically identify the source document by author, date and subject on the "Derived from" line.

5. Declassify On Line. Mark the "Declassify on" line with the declassification instruction from the source document that requires the longest period of classification..

E. MARKING INFORMATION TRANSMITTED ELECTRONICALLY.

Information transmitted electronically by any means, such as message traffic, classified e-mail, must be marked, as would any other classified document, with the following special provisions:

1. The classification line must indicate the highest level of classification double spaced.

2. For information printed by an automated system, overall and page markings may be applied by the system, provided they stand out conspicuously from the text. This may be achieved by surrounding the markings with asterisks or other symbols.

3. Properly completed 'Classified by" and "Derived from" line, declassification and downgrading instructions (when appropriate) must be included in the last line.

4. The following abbreviations may be used:

   a. CLASS for Classified by

   b. DECL for Declassify on

   c. DERV for Derived from

   d. DNG for Downgrade to

5. If multiple sources are the source for derivative classification in an electronic document, the derived from line may indicate "multiple sources" however, the originator must maintain a file copy listing all sources used, until the declassification date.

6. Exhibit 3-10 shows a properly marked document for electronic transmission.

SECRET
(PRECEDENCE) (DATE-TIME-GROUP)
FM USCGC DEPENDABLE
TO CCGDSEVENTEEN JUNEAU AK//MOC//
BT
S E C R E T //N05510//
SUBJ: RECOMMENDATIONS FOR RESOLVING FUNDING PROBLEMS (U)
A. YOUR 081919Z MAY 98
1. **(U)** THE THREE LEVELS OF CLASSIFICATION ARE DOUBLE SPACED WHEN TYPED ON THE CLASSIFICATION LINE.
2. **(S)** PORTION MARKING REQUIREMENTS FOR MESSAGES ARE TH4E SAME AS FOR OTHER DOCUMENTS.
3. **(C)** THE "CLASSIFIED BY" OR "DERIVED FROM" LINE MUST BE INCLUDED IN THE LAST LINE OF THE MESSAGE.
4. **(U)** DECLASSIFICATION MARKINGS ARE ABBREVIATED AS SHOWN BELOW.
DERV: COMDT LTR 5510 5/28/98
DECL: 31 DEC 06
BT
SECRET

EXHIBIT 3-10

F. DERIVATIVELY CLASSIFYING FROM A CLASSIFICATION GUIDE.

1. A classification guide is a document issued by an original classification authority that provides derivative classification instructions. It describes the elements of information that must be protected, and the level and duration of classification.

   a. Portion Markings. Portion mark the classified information incorporated in the derivative document with the level indicated in the classification guide. Mark all other portions, which are unclassified, "(U)".

b. Overall Classification Markings. Conspicuously mark the overall classification at the top and bottom of the derivative document.

c. Derived From Line. The classification authority is the classification guide. Identify the guide on the "Derived from" line. The source for derivative classification is the classification guide.

d. Declassify On Line. Enter the declassification instructions specified in the guide on the "Declassify on" line. When a classification guide contains the declassification instruction "Originating Agency's Determination Required" or "OADR" the derivative classifier shall carry forward:

(1) The fact that the classification guide contains this instruction.

(2) The date of the classification guide.

(3) This marking will permit the determination of when the classified information is 25 years old an, if permanently valuable, subject to automatic declassification under EO 12958.

NOTE: The declassification instruction "Originating Agency's Determination Required" or "OADR" would only be valid for a classification guide which has not yet been updated and was issued before October 14, 1995 (the effective date of EO 12958).

G. CLASSIFICATION EXTENTIONS.

1. An original classification authority may extend the duration of classification for successive periods not to exceed ten years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of the information origin.

2. Revise the "Declassify on" line to include the new declassification instructions, and the identity of the person authorizing the extension and the date of the action.

3. Reasonable attempts should be made to notify all holders of a classification extension.

H. FOREIGN GOVERNMENT INFORMATION.

1. Mark documents containing classified foreign government information with "**This document contains (country of origin) Information"**. See Exhibit 3-11.

2. Mark the portions that contain the foreign government information to indicate the country of origin and the classification level. Substitute the words "Foreign Government Information" and "FGI" in instances in which the identity of the specific government must be concealed.

DERIVATIVE DOCUMENT

SECRET

5510

Dec 23, 1998

Subject: Recommendations for resolving Funding Problems (U)

1. **(ROM-S)** This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses

T. SPERBER
By direction

Derived From: COMDT ltr 5510 dtd 28 May 98
Subj: Funding Problems
Declassify on: December 31, 2006

SECRET
THIS DOCUMENT CONTAINS ROMULAN INFORMATION

EXHIBIT 3-11

I. RESTRICTED DATA.

1. Classified material containing Restricted Data as defined in the Atomic Energy Act of 1954 (as amended) shall be marked as follows:

"**RESTRICTED DATA**"

"This material contains Restricted Data as defined in the Atomic energy act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."

2. The full notice shall be located at the lower left of the cover page beneath the "Classified by" line, in lieu of a "Declassify on" line. The short form of the notice is "RESTRICTED DATA"; the abbreviated form is "RD".

J. FORMERLY RESTRICTED DATA.

1. Classified material containing Formerly Restricted Data as defined in Section 142.d of the Atomic Energy Act of 1954 (as amended) shall be marked as follows:

"**FORMERLY RESTRICTED DATA**"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954."

2. The full notice shall be located at the lower left of the cover page beneath the "Classified by" line, in lieu of a "Declassify on" line. The short form of the notice is "FORMERLY RESTRICTED DATA"; the abbreviated form is "FRD".

K. LETTERS OF TRANSMITTAL.

1. Conspicuously mark an unclassified transmittal document with the highest classification level of any information transmitted by it. Also mark the transmittal

document with an appropriate instruction indicating that it is unclassified when the classified enclosures are removed.

2. If the transmittal document itself contains classified information, mark it as required for all other classified information, except:

    a. Conspicuously mark the top and bottom of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures.

    b. Mark the transmittal document with an appropriate instruction indicating its overall classification level when classified enclosures are removed.

L. CLASSIFICATION MARKINGS ON DIFFERENT TYPES OF MATERIAL.

1. General Provisions. The security classification level, downgrading (if any), derived from, and declassification instructions shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device on classified information other than documents and their containers. If the information cannot be marked, recipients will be provided with written notification of the classification and associated markings. These provisions are referred to below as "classification markings".

2. Charts, Maps and Drawings. Charts, maps and drawings shall bear the appropriate classification marking under the legend, title block or scale, in such a manner as to differentiate between the classification assigned to the document as a whole and any classification assigned to the legend or title itself. The higher of those markings shall be inscribed at the top and bottom of each document. When the customary method of folding or rolling charts, maps or drawings would cover the classification markings, additional classification markings shall be placed as to be clearly visible when the document is folded or rolled.

3. Photographs. Negatives and positives shall be marked with the appropriate classification markings and kept in a case, folder, etc. bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip and single negatives marked with the appropriate classification. Caution must be exercised when using self-processing fold or paper to photograph or reproduce classified information, since the negative of the last exposure may remain in the camera. All component parts of the last exposure shall be removed and destroyed as classified waste or the camera shall be protected as classified information. All prints shall be marked top and bottom on each side with the appropriate classification markings. All separate reproductions of the photograph will show the markings as well.

4. Transparencies and Slides. Applicable classification markings shall be shown clearly on the image of each transparency or slide and on its border, holder or frame. When transparencies or slides are reproduced as a part of hard copy text material, classification markings will be shown below the markings on the image.

5. Videotapes and Motion Picture Films. Classified videotapes and motion picture films shall be marked at the beginning and end of each reel or tape by titles bearing the appropriate classification markings. Such markings shall be visible when projected on the screen. The outer case or cover for reels and tapes shall bear the same classification markings.

6. Recordings. Recordings, sound or electronic, shall contain a the beginning and end, a statement of the assigned classification which will provide adequate assurance that any listener or receiver will know that classified information of a

specified level is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification markings.

7. Microfilm. Microfilms are copies usually produced photographically on transparent or opaque materials in sizes too small to be read by the unaided eye. Accordingly, the assigned classification markings shall be conspicuously marked on the microform

M. **INTELLIGENCE INFORMATION.** The Director of Central Intelligence (DCI) has prescribed control markings for intelligence. These markings shall be used only on intelligence products and for the purposes described. The control markings shall be assigned individually at the time of preparation of intelligence products, in conjunction with security classification markings and other markings specified by this manual. Authorized control markings for intelligence are:

1. "NOT RELEASABLE TO FOREIGN NATIONALS". This marking is used, with a security classification, to identify intelligence that may not be released in any form to foreign governments, foreign nationals, or non-U. S. Citizen without permission of the originator. This marking will be used on intelligence which, if released to a foreign government or national, could jeopardize intelligence sources or methods, or which it would not be in the best interests of the U. S. to release from a policy standpoint, as specifically determined by a Senior Official of the Intelligence Community. Senior officials of the intelligence community are responsible for developing, publishing, and maintaining guidelines for use in determining the foreign releasability of intelligence they collect or produce. These guidelines will be used in assigning this control marking and in responding to inquiries from other agencies on application of this control. The short form of this marking is "NOFORN"; the abbreviated form is "NF".

2. "AUTHORIZED FOR RELEASE TO (name of country/international organization)". This marking is used to identify classified intelligence that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign country(ies) or organization (s) indicated. No other foreign dissemination of the material is authorized without the permission of the originator. This marking shall not be used in conjunction with the "NORFORN" marking, however, when a document has separate portions marked "NF" and at least one portion marked "REL", the overall page marking shall be "NORFORN PORTIONS REL TO (name of country(ies)/international organization(s))". The short form of this marking is "REL TO (abbreviated name of country(ies) or organization)"; the abbreviated form is "REL (abbreviated name of country(ies) or organization)".

CHAPTER FOUR - SAFEGUARDING

A. BASIC POLICY.

1. Commanding officers are ultimately responsible for the proper safeguarding and accountability of all classified information within their command, regardless of its form.

2. Authorized persons having access to classified information are responsible for:

   a. Protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person.

   b. Meeting safeguarding and accountability requirements prescribed by this manual.

   c. Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

3. Valuables, such as money, jewels, precious metals, weapons, narcotics, etc., shall not be stored in the same containers used to safeguard classified material.

4. Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U. S. Government controlled facilities unless otherwise stipulated in treaties or international agreements.

5. Each container used for the storage of classified material shall be designated (but not externally marked) as to the level of classified material authorized to be stored therein. Each container shall be assigned a number or symbol for identification purposes. The number or symbol shall be affixed in a conspicuous location on the outside of the container. Containers with multiple locking drawers shall have each drawer labeled appropriately.

B. DEFINITIONS.

1. Open Storage Area: An area, constructed IAW this chapter, authorized by Commandant (G-CFI) or cognizant security manager for open storage of classified information.

2. Authorized Person: A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

3. Cleared Commercial Carrier: A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

4. Security-in-Depth: A determination by the cognizant security manager that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed open storage areas, and security storage cabinets during non-working hours.

5. Vault: An area approved by the cognizant security manager which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry. A General Service (GSA) approved modular vault may be used in lieu of the above. Vaults shall be equipped with a GSA-approved vault door and lock.

C. STORAGE REQUIREMENTS.

1. Top Secret**:** Top Secret information shall be stored in the following method:

   a. In a GSA-approved security container with **one** of the following supplemental controls:

      (1) The location that houses the security container shall be subject to continuous protection by guard or duty personnel;

      (2) Guard or duty personnel shall inspect the security container once every two hours;

      (3) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

(4) Security-In-Depth when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740. *(Currently, the Mas-Hamilton X-07 and X-08 are the only locks to meet this requirement.)*

2. Secret. Secret information shall be stored by one of the following methods:

   a. In the same manner as prescribed for Top Secret information;

   b. In a GSA-approved security container or vault without supplemental controls.

3. Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

D. SPECIALIZED SECURITY CONTAINERS. When one-drawer GSA-approved security containers are used for storage of classified material; they must be rendered non-portable by attaching them to a permanent fixture. This may be accomplished by welding the safe to the deck or attaching it by bolts through safe's bolt holes in the bottom of the container. *NOTE: Field Safes are prohibited except in aircraft, and then only after security manager approval.*

E. EXCEPTION FROM STORAGE REQUIREMENTS. A class-wide exception to classified storage aboard 378 high endurance cutters has been granted. Exception #5510-E-01-93 is authorized for the safe located in the commanding officer's cabin (compartment #02-104-1&2, stateroom #02-97-1&2-L) subject to the following conditions. The safe shall be inspected and approved (in writing) by the cognizant security manager, a copy of the approval letter shall be retained in the safe and the safe shall only be authorized for storage up to and including secret.

F. INSPECTION OF SECURITY CONTAINERS.

1. Security containers used for the storage of classified material shall be inspected for tampering when any of the following occur:

   a. A security container has been found open and unattended.

   b. The combination is suspected of having been compromised.

   c. A newly obtained container has been received.

2. A repaired security container shall be inspected to ensure it has been repaired to its original state of security integrity.

3. In addition, the CSO shall inspect the accessible exterior of the container at least annually to ensure its integrity. Security Container Records Form, OPNAV 5510/21 shall be used for this purpose.

4. The cognizant security manager shall inspect all containers used for the storage of classified material as part of the biennial evaluation, to ensure only approved containers are being used.

G. COMBINATIONS.

1. The classification of the combination shall be the same as the highest level of classified information that is protected by the lock.

2. Combinations to dial-type locks shall be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination.

3. Combinations shall be changed under the following conditions:

   a. Whenever such equipment is placed into use.

   b. Whenever a person knowing the combination no longer requires access unless other sufficient controls exist to prevent access to the lock.

   c. Whenever a combination has been subject to possible unauthorized disclosure.

   d. When the container is to be used to store material of a higher classification than the clearance level of one or more of the persons who know the current combination.

   e. At least annually.

4. Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the built-in combination lock shall be reset to a standard combination i.e., 50-25-50. Prior to a security container being retired from use, a careful search shall be made inside, behind, and under all drawers to assure that no classified information is inadvertently left in the container.

5. The Security Container Information Form, SF 700, shall be used to record combinations for each security container used to store classified material.

6. In selecting combination numbers, multiples of five, simple ascending or descending arithmetical series and personal data shall not be used. The same combination shall not be used for more than one container.

7. Combinations shall be protected in the manner prescribed based on the level of classification and will be stored in a separate security container.

H. REPAIR OF SECURITY CONTAINERS.

1. The cognizant security manager shall be contacted prior to authorizing a security container to be drilled or cut open. A subsequent report shall be submitted to the cognizant security manager including the following information:

   a. The reason for drilling or cutting open.

   b. Who performed the drilling or cutting open?

   c. Whether the lock or the locking mechanism malfunctioned.

   d. Any other available information regarding the incident.

2. A Security Container Records Form, OPNAV 5510/21, shall be used to record all repairs, modifications; etc. to all security containers storing classified material. The form shall be located in the front of the locking drawer of the security container.

3. Neutralization of lockouts or repair of any damage which affects the integrity of a security container approved for storage of classified information will be done only by appropriately cleared or continuously escorted personnel specifically trained in the approved methods.

4. A GSA-approved security container is considered to have been restored to its original state of security integrity if:

   a. Authorized locks were used as replacements for the original equipment on containers that have been drilled immediately adjacent to or through the dial ring to neutralize the lockout; the drilled hole is repaired with a tapered case-hardened steel rod with a diameter slightly larger than the hole and of such length that when driven into the hole there remains, at each end of the rod, a shallow recess not less than 1/8 inch nor more than 3/16 inch deep to permit the acceptance of substantial welds, and the rod is

welded on the inside and outside surfaces. The outside of the drawer head must be puttied, sanded and repainted so no visible evidence of the hole or its repair remains on the outer surface.

5. When repair results are visible and could be mistaken for marks left in an attempt at unauthorized entry to the container, post a label inside the locking drawer stating details of the repair. Utilize the OPNAV Form 5510/21 for this purpose.

6. If the damage is repaired using methods other than those outlined, limit the use of the container to unclassified material. Permanently mark a notice to this effect on the front of the cabinet.

I. <u>CONTAINER PRECAUTIONS</u>. The following special precautions shall be followed to ensure that adequate security is being provided:

1. Personnel shall be instructed on the proper method of securing the container to ensure it is properly locked.

2. Security containers shall be kept locked when not under the direct observation of the custodian or other authorized persons.

3. Reversible "OPEN"/"CLOSED" signs shall be used as additional reminders on security containers.

4. A Security Container Check Sheet, SF 702, shall be affixed to the container and used each time the container is opened and closed. Completed SF 702 Forms shall be retained for 3 months.

5. All built-in combination locks shall be equipped with a plastic dust cover (Mas-Hamilton X-07/08 locks are exempted).

6. A brief Standard Operating Procedure (SOP) shall be affixed to the outside front of the container, to inform individuals of the steps to be taken if the container is found open. For example, post a guard, do not look through contents of the safe, notify Officer of the Day, etc.

J. <u>GENERAL SECURITY PRECAUTIONS</u>.

1. Classified documents, when removed from storage, shall have a Classified Information Cover Sheet, SF 703, 704 or 705, attached.

2. Preliminary drafts, carbon sheets, plates, computer disks, stencils, notes, worksheets, ribbons and all other items used for processing classified information shall be protected in the same manner as the highest level of classification for which they have been used.

3. A system of double security checks shall be employed to ensure that all classified information is protected at the close of business. These checks will be recorded on the Activity Security Checklist, SF 701. Completed SF 701 Forms shall be retained for 3 months. *Spaces that are occupied on a 24 hour basis (e.g. COMMCENS/OPCENS) are exempt from this requirement.*

4. Units shall meticulously scrutinize their holdings to ensure that they hold only the classified information that they are required or must have for efficient operation. Classified material determined to be excess, superseded or not longer needed will be returned or destroyed as appropriate.

K. EMERGENCY PLANNING.

1. Emergency Action Plans (EAP) shall be developed for the securing and removal of classified information in case of natural disaster or civil disturbance. Such plans shall establish detailed procedures and responsibilities for the securing and removing of classified information so that it does not fall into unauthorized hands. The EAP shall indicate what information is to be secured or removed and shall provide for securing the information and/or removing the information from the area. In addition, shore units located outside the 50 states and all mobile units shall have a destruction bill included in the EAP.

2. In developing an EAP, each unit must initially review its vulnerability to situations, which could result in the compromise of classified information.

   a. An evaluation of vulnerability should include a review of such items as:

      (1) The size and composition of the unit.

      (2) Existing physical security measures.

      (3) The location of the unit and the degree of control it or other military authority may exercise over security (e.g., shipboard units, units located within Federal office buildings, and units housed within leased private buildings vary in their control over security measures).

      (4) The classification level and amount of classified information held by the unit.

      (5) The effect of disruption on the unit's mission.

(6) Local conditions relative to incidents that may erupt into an emergency situation.

b. Once a vulnerability evaluation has been made practical measures and procedures shall be established to strengthen weaknesses and to provide planning for the safeguarding of classified information. Measures taken as part of emergency planning should include:

(1) Providing for the protection of classified information in a manner that will minimize the risk of loss of life or injury to personnel.

(2) A means of inventorying all classified information to be removed from the unit.

(3) Designating persons authorized to make the decision that an emergency condition exists and to implement the EAP.

(4) Determining the most effective use of security personnel and equipment. This should include consideration of removing classified information to more secure storage areas within the unit.

(5) Designating additional unit personnel and equipment that may be used in support of normally assigned security forces.

(6) Coordinating with local law enforcement agencies and other nearby military units for the support that is required.

(7) Designating alternate safe storage areas outside of the unit, which classified information, could be evacuated when it is considered that the unit would not be able to employ the measures necessary for its protection. Where evacuation is planned, arrangements should be made for packaging supplies and moving equipment.

(8) Educating and training all unit personnel regarding their responsibilities during an emergency. Additional instruction and training should be given to security forces and augmenting personnel to ensure familiarity with the EAP.

(9) Establishing procedures to dismiss nonessential personnel should conditions warrant.

(10) Determining the action to be taken to divert attention from the most sensitive material where loss of control over some classified material is certain.

(11) Measures to be taken as part of emergency planning may include a provision for identifying intruders and recording their actions through observation for later use in damage assessment and possible prosecution.

(12) Establishing the requirement to inventory classified information as soon as possible after the emergency to determine accountability and to report any compromise.

c. Drills shall be conducted and documented semiannually to ensure that those responsible are familiar with the EAP. Drills shall be used to evaluate the effectiveness of the plan and the resources required to carry it out.

L. RESTRICTED AREAS.

1. All classified spaces shall be designated "Restricted Area", and have warning signs posted as set forth in the Physical Security Program, COMDTINST M5530.1 (series). The cognizant security manager shall designate these areas in writing. Authorization for designation of such areas is Title 18 U.S.C. 1382. Restricted areas are defined as follows:

a. Exclusion Area. An exclusion area is the most secure type of restricted area. It may be within less secure types of restricted areas. Access to the exclusion area constitutes, or is considered to constitute, actual access to the security interest or asset.

b. Limited Area. A limited area is the second most secure type of restricted area. It may be inside a controlled area, but is never inside an exclusion area Uncontrolled or unescorted movement could permit access to the security interest or asset.

c. Controlled Area. A controlled area is the least secure type of restricted area. It may serve as a buffer zone for exclusion and limited areas, thus providing administrative control and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to the security interest or asset.

M. UNAUTHORIZED ACCESS.

1. When an unauthorized individual enters a Restricted Area, he/she shall be apprehended and immediately brought before proper authority where he/she shall be searched and interrogated. If it is a first offense and the offense appears not to have been willful, the offender shall be warned against repetition and released. Where it appears that the unlawful entry was made with the intent to do harm to the national security, the nearest office of the Federal Bureau of Investigation (FBI) shall be notified, and the offender shall be delivered without delay to the nearest United States Marshal with a written statement of the facts, the names and addresses of witnesses, and such pertinent exhibits as may be available. In all cases any notes, photographs, sketches, pictures, drawings, maps, graphic representations or material found in his/her possession shall be confiscated.

2. Violators of restricted areas who are subject to military law will be dealt with under the appropriate provisions of the Uniform Code of Military Justice.

3. A report shall be submitted through the chain of command to the cognizant security manager with an information copy to Commandant (G-CFI) concerning each case of a deliberate violation of a restricted area. The report will include a brief summary of all the facts and the commanding officers determination of damage.

N. CLASSIFIED SPACES.

1. A classified space is a restricted area in which classified information is routinely processed, formulated, discussed or openly displayed. Conference rooms, classrooms, Operations Centers (OPCEN), Communications Centers (COMMCEN), Security Management and Law Enforcement Offices may be designated as a Classified Space. If the designation is approved by the security manager command funding is required.

2. Classified information shall be stored only under those conditions described in chapter 4 of this manual. The requirements for safeguarding classified information shall be strictly adhered to.

3. When the need exists to establish a classified space, all plans shall be coordinated with the cognizant security manager prior to construction/modification. Once constructed, spaces shall be inspected and approved by the security manager in writing.

4. The physical security standards in this section comprise only one of the elements of a classified space. There are also communications, technical, and TEMPEST security considerations. Additional guidelines and

physical security standards are published separately by responsible program managers. The cognizant security manager should be consulted to ensure all physical security standards are addressed.

5. Office spaces are defined as those administrative spaces, e.g. personnel offices, training offices, security control points, etc. that are not normally used in the conduct of classified operations. As such, these physical security requirements do not apply to these spaces. Emphasis shall be placed on access control and individual security responsibilities.

6. Walls, Floors and Ceilings. Walls, floors and ceilings shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry; all construction shall be done in a workmanlike manner, properly finished, and/or painted. This includes areas above a false ceiling and under a raised floor. Workmanlike manner means that all cracks, holes, and openings on the interior and exterior of the space are permanently sealed, properly finished, or painted. Painting and paneling are optional.

7. Windows. If windows exist and afford optical surveillance of personnel, documents, equipment or activities, they must be made opaque, equipped with drapes, or otherwise totally obscured to preclude surveillance. Ready accessible windows shall be protected against forced entry with hardened steel bars or an intrusion detection system (IDS). Windows 18 feet or more above ground level and 14 feet or more away from structures are not considered to be accessible.

8. Other openings.

   a. All air vents, ducts, pipes, and similar openings (less than 90 square inches) may require acoustical protection by either sound baffles or a sound masking system

   b. Openings greater than 90 square inches that enter or pass through a classified space shall be protected with either hardened steel bars, grills, IDS, and/or approved commercial sound baffles.

      (1) If bars are used, they shall be ½ inch in diameter, mounted 6 inches on center vertically and horizontally, and welded at all intersections. If one dimension of the duct measures less than 6 inches, bars are not required.

      (2) If grills are used, they shall be nine gauge expanded steel.

      (3) If commercial sound baffles are used in lieu of bars or grills, the baffles or wave forms shall be metal and

permanently installed (no farther apart than 6 inches in one dimension). A deviation of ½ inch in vertical and/or horizontal spacing is authorized.

(4) An access port shall be installed inside the space to allow visual inspection of the protected opening. A padlock shall secure the access port or other approved locking device.

c. All vents and ducts for classified spaces which electronically process Top Secret shall have a 6 inch non-conductive section (a piece of dissimilar material, e.g., canvas or rubber, which is unable to carry electric current) installed at the interior perimeter of the space. The non-conductive section shall begin at the space interior perimeter and extend inward. There shall be no exposed metallic ductwork between the space interior perimeter and the non-conductive section.

d. Pipes may enter and leave the classified space perimeter carrying water, waste, air, steam, cooling and heating fluids, or to provide a vacuum supply. All metallic pipe installations shall be modified to prevent them from being used to exploit security weaknesses within the space. Non-conductive pipes do not require dielectric protection treatment.

(1) Fire suppression system pipes shall be electrically grounded at the entrance and exit points of the space.

(2) Waste pipes that do not go into the earth inside the space shall be electrically grounded at the entrance and exit points of the space.

(3) Air, vacuum, cooling and heating fluid pipes shall be electrically grounded at the entrance and exit points of the space, or is equipped with a non-electrically conductive section approximately 6 inches in length. The non-conductive section shall begin at the space interior perimeter and extend inward. There shall be no exposed metallic pipe between the space interior perimeter and the non-conductive section.

(4) Steam, high pressure air, miscellaneous and industrial system supply pipes shall be individually treated in the most effective manner designed to electrically ground them at the entrance and exit points of the space.

9. Doors. There shall be a single, controlled entrance to classified spaces. When safety or other considerations require more than one door, only one of the doors shall be used as the controlled entrance. Other doors shall be of equal construction as the entrance door and secured from the inside with either sliding 1-inch throw deadbolts or panic hardware to enable rapid egress in the event of an emergency. The entrance door and frame shall be of the acoustical type and shall meet the appropriate sound attenuation. The entrance door shall also be equipped with a pneumatic closer, group 1R combination lock, and an appropriate strike and drill resistant 1/8-inch hard plate installed between the lock and the door. The group 1R lock may be left in the open position if a convenience lock is installed for normal access controls. However, when the space is unmanned or in the event of emergency evacuation, the group 1R lock must remain in the locked position. All perimeter door hinges located on door exteriors shall be of the non-removable type with hinge pins peened or welded to preclude removal. All perimeter doors shall be equipped with Balanced Magnetic Switches (BMS).

10. Sound Attenuation. The term "sound transmission class" (STC) is used in architectural acoustics to describe the transmission attenuation afforded by various wall materials and other building components. The classification applies to all perimeter walls, floors, ceilings, doors, windows, vents, ducts and any other openings exposed to uncontrolled areas. An STC 45 is required for Top Secret spaces. This means that anywhere outside of the secure area, loud speech can be faintly heard, but is not understood. Normal speech is inaudible. For spaces Secret and below, a minimum STC 40 is required. This means that loud speech can be heard, but is hardly intelligible. Normal speech can be heard faintly, if at all.

11. Telephones and Intercom Equipment. Telephone instruments shall be kept to a minimum. They shall be equipped with a push-to-talk handset. Utilization of Secure Telephone Units (STU IIIs) or telephone security group (TSG) approved telephone instruments/devices are strongly recommended. All incoming/outgoing telephone cables and wiring, to include those used for IDS's, shall enter the space through one common opening and be placed under control. All incoming/outgoing telephone and IDS wiring shall be accounted for by status (active/inactive), exact use (data, voice, or IDS), and by telephone/extension/circuit number. This accounting shall be updated whenever the status of a pair of wires is changed. All excess wiring shall be removed, stripped or bout together and grounded inside the space to a ground point not associated with equipment requiring TEMPEST protection. Radio frequency (RF) filters or optical isolators may be required if classified information is electronically processed. RF filters/isolators may be required, based on an individual assessment by the cognizant TEMPEST authority.

12. Intrusion Detection Systems (IDS). The Physical Security Manual, COMDTINST M5530.1 (series) outlines the basic IDS requirements. Provisions of this section supplement those requirements. Unless continuously manned, classified spaces shall be alarmed with interior alarm sensors to detect unauthorized entry or any attempt to breach the space. A unit's Emergency Action Plan should outline specific procedures in the event of emergencies, evacuations, etc.

13. Sound Masking. A sound masking system provides a programmed cover (not radio or commercially programmed) to effectively mask electronic eavesdropping techniques and helps maintain sound attenuation. These systems may be installed in classified spaces, but shall be approved by the cognizant security manager prior to installation.

CHAPTER SIX – ACCESS, ACCOUNTABILITY AND CONTROL SYSTEM

A. **ACCESS.** The dissemination of classified information, by any means, shall be limited to persons whose official duties require knowledge or possession of the information. **No one has a right to have access to classified information solely by virtue of rank or position**. Three criteria must be met prior to the granting of access: security clearance, need to know, and a properly executed non-disclosure agreement.

1. Security Clearance. Security clearance procedures for Coast Guard military personnel are contained in the Coast Guard Military Personnel Security Program, COMDTINST M5520.12 (series).

2. Need to know. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient.

3. A properly executed SF-312, Non Disclosure agreement must be on file.

B. **ACCOUNTABILITY AND CONTROL SYSTEMS.** Accountability of classified information is essential to maintaining a history of WHAT YOU HAVE, WHERE IT IS, and WHO HAS IT. Through effective accounting procedures it must be possible to trace the movement and detect the loss of classified information in a timely manner.

1. All Top Secret and Secret information shall be strictly accounted for and covered by a continuous chain of signature receipts. There is no requirement for a continuous chain of signature receipts for Confidential material. However, this chapter represents the **MINIMUM** requirements for accountability and control. Commands are encouraged to implement additional controls they deem appropriate.

2. A number of systems have been established to control and account for classified information:

   a. Communications Tactical (COMTAC) Publication Library (CPL). COMTAC publications are certain Communication tactical Doctrine, Warfare, Allied, and NATO publications sponsored by the Office of the Chief of Naval Operations. COMTAC publications shall be accounted for in accordance with the

procedures set forth in COMTAC Publications Index, COMDTINST M2600.1 (series).

b. Communications Security (COMSEC) Material System (CMS). CMS is a system to ensure the proper distribution, control, security, and accountability of COMSEC material used throughout the U.S. Navy, Marine Corps, and Coast Guard to provide cryptographic security for national security related information. CMS material shall be accounted for in accordance with the procedures set forth in Communications Security Material System, CMS 1 (series) and CMS 21 (series).

c. North Atlantic Treaty Organization (NATO) Information. NATO classified information may be military, political or economic information. Such material may originate in NATO itself or it may be received from member nations or other international organizations. NATO material shall be accounted for in accordance with the procedures set forth in the U.S. Coast Guard NATO Security Manual, COMDTINST M5500.19 (series).

d. Classified Material Control (CMC) System. All other types of classified material that do not fall under a specific accountability system shall be accounted for in the CMC system as set forth in this manual.

C. **SECURITY CONTROL POINT (SCP).** One SCP, operated by the Classified Material Control Officer (CMCO), shall be established within each unit which has a requirement to handle classified information. All incoming and outgoing classified information shall be processed through the SCP with the following exceptions: Sensitive Compartmented Information (SCI) material; CMS material; COMTAC publications; classified messages that are handled, processed and stored within secure telecommunications spaces; and as exempted in paragraph 10-F. The SCP shall be designated in writing within the local unit information security plan.

D. **DOCUMENT CONTROL STATION (DCS).** In larger units with a significant volume of classified material and where the SCP serves many elements, each element which has or will have custody of classified material shall establish a DCS run by a Document Control Station Officer (DCSO). Organizationally, this station may be established at the office, division, staff or lower level depending upon the circumstances.

E. ACCOUNTABILITY RECORDS.

1. There is no requirement for accountability records for material classified Confidential. As stated in paragraph B above, this policy represents the minimum requirements. Commands may implement additional controls as they deem necessary.

2. Adequate records shall be maintained for all Top Secret and Secret information and retained for five years after final disposition. These records shall be maintained at the SCP for any accountable information, which is received, generated, reproduced, transmitted, downgraded or destroyed. A Classified Document Control Log (CG-4819) or suitable substitute shall be used for this purpose.

3. The Document Control Log maintained at the SCP shall, at a minimum, reflect the following:

   a. Date of receipt and date of origination.

   b. Unit from which received or by which originated.

   c. Classification level of the material.

   d. A brief unclassified description of the material.

   e. The date of declassification or downgrading.

   f. Control number assigned. Each copy of a classified document or item shall have its own control number. Copy numbers will not be used as part of the control number.

   g. Information indicating the location or local holder of the material. (Local holders/custodians shall have some form of signature receipt on file acknowledging that they have custody of the material).

   h. Disposition and date for all material destroyed, downgraded, declassified or dispatched outside of the unit.

4. The Document Control Log maintained at the DCS shall, at a minimum, reflect the following:

   a. Classification level of the material.

   b. Control number assigned.

c. Disposition and date for all material destroyed, downgraded, declassified or dispatched outside of the DCS.

5. Accountability records shall also contain signed receipts and destruction reports. Signed receipts and destruction reports shall be retained for four years after final disposition.

F. EXCEPTIONS FROM ACCOUNTABILITY.

1. Secret messages: Secret message traffic sent or received at a unit is exempted from accountability under the following conditions:

   a. The message remains within the command that originated or received the message.

   b. Account for all messages and copies transferred or distributed outside of the command.

   c. Only those Secret messages determined operationally required should be reproduced, following the requirements of chapter 7 of this manual. Reproductions shall be clearly marked "REPRODUCED FOR" along with the individual's name and/or office name.

   d. Ensure that all individuals who are authorized to request and receive reproductions of Secret messages within the command have storage capability approved for Secret material, and are briefed on their responsibilities with regard to safeguarding and destruction.

   e. Establish written procedures approved by the Command Security Officer (CSO) and commanding officer to ensure compliance with the above requirements.

2. Electronic Processing: Units that electronically process Secret information, (including e-mail), within a designated restricted area that meets the security requirements of a classified space in accordance with this manual, are authorized an exception from the requirement to account for that Secret material under the following conditions:

   a. Account for Automated Data Processing (ADP) storage media.

   b. Account for Secret material that is transferred or distributed outside the classified space (see paragraph F.1. for secret message traffic).

c. When a classified ADP system is used, print only that material that is operationally required to be "hard copy". Conspicuously mark the "hard copy" to indicate the unit and/or office printing the copy.

d. Limit the number of personnel authorized to print classified material from a classified ADP system.

e. Ensure that all Secret material is destroyed by an approved method.

f. Ensure quarterly refresher security briefs are conducted and documented for all personnel working in the classified space. The intent is to increase security awareness to compensate for these relaxed security requirements.

g. Establish written procedures approved by the Command Security Officer (CSO) and commanding officer to ensure compliance with the above requirements. These procedures may be included in the unit's information security plan discussed in this manual.

h. This exception does not apply to any other accountable Secret material stored within the classified space.

G. <u>RECEIPT OF CLASSIFIED MATERIAL</u>. The unit shall provide written procedures for the handling of incoming classified material. When a unit receives incoming mail, bulk shipments, and items delivered by messenger, the following controls shall be implemented:

1. All classified material shall be delivered promptly to the SCP or properly safeguarded in accordance with this manual, until delivery to the SCP can be effected.

2. All Registered, USPS Express mail and contract (FEDEX, etc.) overnight delivery packages shall be delivered unopened to the SCP and protected as Secret material until determined otherwise.

3. All personnel who open Official Mail (of any sort) shall be directed to immediately deliver any classified material to the SCP. Outer wrappers along with the UNOPENED inner wrapper shall be delivered to the SCP. If an individual opens mail which is not correctly packaged causing exposure by an uncleared or unauthorized individual, the material will be delivered to the SCP and the CSO will be notified. The CSO will investigate and submit a report of incident involving classified material outlined in chapter 12 of this manual.

4. All incoming packages containing classified material shall be inspected for tampering. If tampering is discovered, it shall be reported to the CSO

who shall conduct such inquires as are necessary. The contents of the package shall be checked against the enclosed receipt.

5. Incoming classified information that does not fall under the CMC system shall be processed in accordance with the procedures established for that type of material.

H. RECORD OF DESTRUCTION.

1. An accurate record of destruction of classified material is as important as its destruction. Proper accounting procedures, together with accurate records of destruction, provide evidence of the proper disposition of classified material. Records of destruction shall be retained for four years.

2. A record of destruction is required for Top Secret and Secret classified material. The destruction record shall indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness. Both individuals must have personal knowledge of the actual material destroyed. If applicable, the official authorizing the destruction shall also sign the record. Either the control log or a separate destruction report may be used for this purpose.

3. Records of destruction are not required for Confidential material or material exempted from accountability in Paragraph F.1.

I. CHANGES IN ACCOUNTABILITY.

1. Lost Material. Whenever classified material has been determined to be lost or unaccounted for through an incident or investigation, the unit will obtain authority for removal from accountability. After reviewing the incident and closing the case, the area/district security manager will authorize the removal. Once authorized to remove from accountability, annotate records to show the date, reason and authority for terminating accountability.

2. Material previously reported lost. When classified material is found that was previously reported as lost, an incident involving classified material will be submitted in accordance with chapter 12 of this manual. The unit will immediately reestablish accountability for, or indicate the disposition of, the material on the SCP accountability records.

J. TOP SECRET DISCLOSURE RECORDS. A disclosure record of all persons who are afforded access (visual, oral, record copies, etc.) to Top Secret information (except safe combinations) shall be maintained. This record shall show the names of all individuals given access and the date of such access. To comply with this requirement, a Top Secret Disclosure Record Sheet (CG-4764A) shall be attached to all Top Secret information in document form. For access given orally, a log listing the required information shall be maintained. Records shall be retained for five years from the date of final disposition.

K. INVENTORY REQUIREMENTS.

1. Two appropriately cleared individuals shall conduct inventories. One of the individuals may be the control officer for the material. However, the other individual must be a disinterested party not involved in the operation of the account.

2. An inventory is a visual sighting of each item of accountable material. All documents held shall be checked to ensure that they are entered into accountability and all documents entered into accountability shall be sighted, including those items signed out on local custody. If no disposition can be determined, an incident involving classified material shall be submitted in accordance with chapter 12 of this manual.

3. All Top Secret holdings shall be inventoried upon change of custodian or semiannually. Semiannual inventories may be combined with change of custodian inventories. Accountability records shall also be reviewed for accuracy and continuity. See paragraph M.2. For a complete listing of required page checks.

4. All secret holdings shall be inventoried upon change of custodian or annually. Annual inventories may be combined with change of custodian inventories. In those instances where exceptionally large holdings (more than 500 control numbers) make conducting an annual inventory difficult, commands may complete the inventory of Secret material over a 3 month period. An inventory is not required for material authorized for an exception to the accountability requirements listed in paragraph F. Top Secret material must be inventoried semi-annually, one of which may be conducted in conjunction with the scheduled annual inventory of Secret material.

5. The unit shall retain a record of all inventories for a period of at least 5 years. An inventory and a report of the results, including any discrepancies discovered, shall be forwarded annually to the cognizant security manager via the commanding officer. Although an inventory of Top Secret holdings is required on a semi-annual basis, a written report to the cognizant security manager is only required annually unless

discrepancies are discovered. Although the Top Secret inventory is only reported annually, local documentation of all inventories must be maintained at the unit as described above.

6. Upon change of custodian, all classified material shall be transferred to the new custodian. A joint inventory shall be conducted, accounting for each item. Both parties shall sign the report.

L. CHANGES AND CORRECTIONS. The custodian, under the guidance of the CMCO, shall be responsible for the entry of all changes and corrections to the material in their custody. Exhibit 6-1 is a sample Publication Change Checklist and shall be used for all changes entered. Completed checklists shall be retained until the publication is destroyed or superseded.

M. PAGE CHECKS.

1. A proper page check involves visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable) and ensuring that the page is from the correct change. In the absence of a list of effective pages, the document shall be examined for continuity. After each page check, the individual shall sign the page check record (except for page checks prior to destruction). If one does not exist, a page check record shall be produced locally and kept with the publication. The record shall identify the publication, the name of the individual conducting the page check and discrepancies noted and the date of the check.

2. Page checks shall be conducted on the following occasions:

	Top Secret	Secret	Confidential
Initial receipt	Yes	Yes	Yes
Page change	Yes	Yes	Yes
Change residue	Yes	Yes	Yes
Change of custodian	Yes	Yes	No
Inventory	Yes	No	No
Destruction	Yes	Yes	No

N. WORKING PAPERS.

1. Working papers are documents, including drafts, notes, photographs, computer media, etc. accumulated, created or received electronically to

assist in the formulation and preparation of a finished document. Classifying as working papers is not intended as a way around the original classification procedure or temporary classification. Working papers produced by a unit, which contain classified information, shall be:

a. Dated when created.

b. Marked with the highest classification of any information contained in the document.

c. Protected in accordance with the classification assigned.

d. After 30 days, material classified as working papers must be destroyed or correctly classified by an original classification authority.

2. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain Top Secret information or are:

a. Released by the originator outside the unit or transmitted electronically.

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

c. Filed permanently.

O. **MAGNETIC/OPTICAL MEDIA.** For accountability purposes each item of magnetic or optical media containing classified information shall be accounted for as a single document. Each document, file or other piece of information stored within the magnetic media shall not be accounted for separately unless it is further printed or reproduced. However, a printed list of documents contained on the disk or CD (except those distributed from another agency) shall be maintained to assist in a damage assessment if the media is subjected to a possible compromise

P. **CLASSIFIED MATERIAL IS NOT PERSONAL PROPERTY.** Classified information is always official information and never personal property. Confusion sometimes arises about classified notes from a training course or conference. As classified material, they are official information, which must be safeguarded, transmitted and destroyed in accordance with this manual. Classified notes cannot be removed from the unit without the commanding officer's permission. Classified notes shall not be considered as working papers but, as official information for which the unit is responsible, they must be transmitted by one of the means authorized for transmittal of classified material and eventually destroyed by authorized means. When an individual leaves a unit,

the unit may officially transfer his/her notes to a new unit where they will again be available for his/her use.

CHAPTER EIGHT – TRANSMISSION OF CLASSIFIED MATERIAL

A. <u>POLICY</u>.

1. Classified material shall be transmitted either in the custody of an appropriately cleared individual or by an approved system or courier, or in accordance with the provisions of this chapter.

2. The term transmission refers to any movement of classified material or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation is not particularly significant.

3. The carrying of classified material across national borders is not permitted unless arrangements have been made that will preclude customs, postal, or other inspections. In addition, foreign carriers may not be used unless the U. S. escort has physical control of the classified material.

B. <u>TOP SECRET TRANSMISSION</u>. Neither the normal mail or messenger system of a unit nor postal and commercial delivery services are authorized for the transmission of Top Secret material. Top Secret material shall only be transmitted by:

1. Defense Courier Service (DCS).

2. Department of State Courier System.

3. Appropriately cleared Coast Guard military and civilian personnel specifically designated as a courier.

4. Telecommunications systems specifically approved for transmission of Top Secret material.

C. <u>SECRET TRANSMISSION</u>. Transmission of Secret material may be effected by:

1. Any of the means approved for the transmission of Top Secret, except that Secret material other than that containing crypptological information, may be introduced into the DCS only when the control of such material cannot otherwise be maintained in U. S. custody. This restriction on use of the DCS does not apply to Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) material. When the Department of State Courier System is to be used for transmission of Secret material, the Secret material shall be sent by registered mail to the State Department Pouch Room.

2. Appropriately cleared Coast Guard military and civilian personnel specifically designated as a courier.

3. U. S. Postal service (USPS) registered mail within and between the 50 United States and its Territories.

4. USPS Express Mail Service may be used between Coast Guard units and contractors within and between the 50 United States and its Territories. USPS Express Mail is authorized only when it is the most cost effective method or when time/mission constraints require it. The package shall be properly prepared for mailing. The USPS Express Mail envelope shall not serve as the outer wrapper. Under no circumstances shall the sender execute the "WAIVER OF SIGNATURE AND INDEMNITY" section of the USPS Express Mail Label for classified material. This action can result in drop-off of a package without the receiver's signature and possible loss of control.

5. When an urgent requirement exists for overnight delivery within the 50 United States and its Territories, the commanding officer may authorize the CSO to use the current holder of the General Services Administration contract for overnight delivery of material for the Executive Branch. Any such delivery service must be U. S. owned and operated, provide automated in-transit tracking of the package and ensure package integrity during transit. The sender is responsible for ensuring that an authorized person will be available to receive the delivery. The package may only be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO and Foreign government information shall not be transmitted in this manner.

6. Outside of the area described in paragraph 3 above, Secret material may be moved by USPS registered mail through Army, Navy or Air Force Postal Service facilities provided that the material does not pass through a foreign postal system or any foreign inspection, or via foreign airlines. The material must remain under U. S. control. Special care shall be taken when sending classified material to U. S. activities overseas. If the material is introduced into a foreign postal system, it has been subjected to compromise.

7. USPS and Canadian registered mail with registered receipt between U.S. Government and/or Canadian government installations in the U. S. and Canada.

8. Within U. S. boundaries only, qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the National Industrial Security Program. This method is authorized only when the size, bulk, weight, nature of the shipment or escort considerations make the use of other means impractical.

9. Other carriers under escort of appropriately cleared personnel. Carriers included are government and government contract vehicles, aircraft, ships of the U. S. Navy, civil service manned U.S. Naval Ships, and ships of U. S. Registry.

Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U. S. citizens may be designated as escorts provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period if stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment which is not accessible to any unauthorized persons aboard, or loaded in specialized shipping containers, including closed cargo containers.

10. Telecommunications systems specifically approved for the transmission of Secret material.

D. **CONFIDENTIAL TRANSMISSION.** Transmission of Confidential material may be effected by:

1. Any of the means approved for the transmission of Secret material.

2. USPS registered mail for:

   a. Confidential COMSEC, NATO and other special category material.

   b. Other confidential material to and from Fleet Post Office (FPO) or Army Post Office (APO) addressees located outside the U. S. and its Territories.

   c. Other addressees when the originator is uncertain that there location is within the U. S. boundaries. Use of return postal receipts is not authorized. If considered desirable, a document receipt may be used.

   d. When the sender deems it necessary to ensure adequate protection of the classified material.

3. USPS First Class mail between Coast Guard and Departments of Defense and Transportation component locations anywhere in the U. S. and its Territories. However, The outer envelope/wrappers of such Confidential material shall be marked “FIRST CLASS”, and endorsed “RETURN SERVICE REQUESTED”

4. Certified or, if appropriate, registered mail shall be used for material directed to DOD and Coast Guard contractors and to non-DOD or non-DOT agencies of the Executive Branch.

5. Within U. S. boundaries, commercial carriers that provide a Signature Security Service (SSS). This method is authorized only when the size, bulk, weight, nature of shipment, or escort considerations make the use of other methods impractical.

6. In the custody of commanders or masters of ships of U. S. registry who are U. S. citizens. Confidential material shipped on ships of U. S. registry may not pass out of U. S. Government control. The commanders or masters must give and receive classified material receipts and agree to:

   a. Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded; and

   b. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

E. TRANSMISSION TO FOREIGN GOVERNMENTS.

1. Subsequent to a determination by Commandant (G-CFI) that classified material may be released to a foreign government; the material shall be transferred between authorized representatives of each government in compliance with the provisions of this chapter. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by Commandant (G-CFI) prior to release of the material. Classified material shall be transmitted only:

   a. To an embassy or other official agency of the recipient government which has extraterritorial status, or

   b. For on-loading aboard a ship, aircraft or other carrier designated by the recipient government at the point of departure from the U. S., or its Territories or possessions, provided that at the time of delivery a duly authorized representative of the recipient government is present at the point of departure to accept delivery to insure immediate loading, and to assume security responsibility for the classified material.

2. Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee. This written designation shall contain assurances that such person has a security clearance at the appropriate level and that the person will assume full security responsibility for the material on behalf of the foreign government. The recipient shall be required

   to execute a receipt for the material, regardless of the level of classification.

3. Each contract, agreement or arrangement, which contemplates transfer of U. S., classified material to a foreign government within the U. S., or its Territories, shall designate a point of delivery in accordance with paragraph 8-E-1-a or 8-E-1-b. If delivery is to be made at a point described in paragraph 8-E-1-b, the contract, agreement or arrangement shall provide the U. S. Government storage, or storage by a cleared contractor at or near the delivery point, so that the U. S. classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading. Any storage facility used or designated for this purpose must afford the U. S. classified material the protection required by this manual.

4. If U. S. classified material is to be delivered to a foreign government within the recipient country; it shall be transmitted in accordance with this chapter. Unless a designated or approved courier or escort accompanies the material, it shall, upon arrival in the recipient country, be delivered to a U. S. Government representative who shall arrange for transfer to a duly authorized representative of the recipient foreign government.

F. <u>CONSIGNOR-CONSIGNEE RESPONSIBILITY FOR SHIPMENT OF BULKY MATERIAL</u>. The consignor of a bulk shipment shall:

1. Normally, select a carrier, which will provide a single line service from the point of origin to destination, when such service is available.

2. Ship packages weighing less than 200 pounds only in closed vehicles.

3. Notify the consignee, of the nature of the shipment (including level of classification) the means of shipment, the number of seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance of arrival of the shipment. Advise the first transshipping activity that, in the event the material does not move on the conveyance originally anticipated, the transshipping activity should so advise the consignee with information of firm transshipping date and estimated time of arrival. Upon receipt of the advance notice of shipment of classified material, consignees and transshipping activities shall take appropriate steps to receive the classified shipment and to protect it upon arrival.

4. Annotate the bills of lading to require the carrier to notify the consignor immediately, by the fastest means possible, if the shipment is unduly delayed enroute. Such annotations shall not, under any circumstances, disclose the classified nature of the shipment. When seals are used, annotate substantially as follows:

"DO NOT BREAK SEALS EXCEPT IN EMERGENCY OR UPON AUTHORITY OF CONSIGNOR OR CONSIGNEE. IF BROKEN, APPLY CARRIER'S SEAL

AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE".

5. Require the consignee to advise the consignor of any shipment not received more than 48 hours after the estimated time of arrival furnished by the consignor or transshipping activity. Upon receipt of such notice the consignor shall immediately trace the shipment. If there is evidence that the classified material was subject to compromise, the procedures set forth in chapter 12 of this manual for reporting incidents involving classified information shall apply.

G. TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL. COMSEC material shall be transported in accordance with Communications Security Material System, CMS 1 (series)/CMS 21 (series).

H. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION. Classified material shall be properly prepared for transmission to protect it from unauthorized disclosure and to show evidence of tampering.

1. Classified material shall be packaged in opaque inner and outer sealed envelopes, wrappings, or cartons.

2. Inner Cover. Written material shall be folded or packed so that the classified text is not in direct contact with the inner cover. The inner cover shall be marked to indicate the highest classification of the material contained and other warning notations as appropriate. The inner cover shall be addressed to the official government activity or cleared contractor and not an individual. *For units that have internal routing symbols, the internal routing symbol or organizational component within the receiving facility shall be placed on the inner envelope only*. The marking **"TO BE OPENED ONLY BY THE CLASSIFIED MATERIAL CONTROL OFFICER"** shall be affixed to the inner envelope. Markings on the inner cover shall not show through the outer cover. The receipt shall be attached to or enclosed in the inner cover. It shall be signed and dated by the receiving unit and promptly returned to the sending unit.

3. Outer Cover**.** The outer cover shall be addressed to the official government unit or cleared contractor and not to an individual. No attention line or internal routing symbol shall be shown on the outer cover. The outer cover shall have no classification markings or any other indication that classified information is enclosed. The outer cover of Confidential material being transmitted by USPS First Class mail shall be marked "Postmaster: Do not forward, return to sender," and "First Class" or "Priority Mail" as appropriate. When classified material is hand-carried outside a unit, a locked briefcase may serve as the outer cover or wrapper.

4. Whenever the classified material being transmitted is too large to prepare as above, it will be enclosed in two opaque sealed containers, such as boxes or heavy wrappings, or prepared as follows:

   a. If the classified material is an internal component of a packageable item of equipment whose outside shell or body is not classified and completely shields the classified aspects of the item from view, the shell or body may be considered as the inner cover.

   b. If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, the outside shell or body of the item may be considered as the outer cover provided the shell or body is not classified.

   c. If the classified material is not reasonably packageable and the shell or body is classified, drape it with an opaque covering that will conceal all the classified features and secure the covering in such a manner as to prevent inadvertent exposure of the item.

   d. Specialized shipping containers, including closed cargo transporters, may be used in lieu of the packaging requirements listed above and are considered the outer cover.

   e. The assigned classification and the address of the consignee shall appear on or be attached to the inner covering, if one is used. The outer cover shall bear the address of both the consignor and consignee. Under no circumstances will the outer cover or the shipping document attached to the outer cover reflect the classification of the contents.

   f. Containers shall be inspected prior to release to ensure that they have been constructed, strapped, and otherwise prepared, including the use of seals when appropriate, to provide necessary protection during shipment.

5. Material used for packaging shall be of such strength and durability so as to provide protection in transit and to prevent items from breaking out of the covers. Packages and envelopes shall be sealed with tape which will retain the impression of any postal stamp (transparent tape, electrical tape and masking tape do no retain a postal seal and shall not be used). Carefully applied brown paper sealing tape is sufficient for inner and outer covers. Packages shall be inspected prior to shipment to insure proper preparation.

6. During transfer at sea, classified material shall be placed in weighted bags to ensure prompt sinking in case of loss into the sea during transfer.

I. RECEIPT SYSTEM.

1. Top Secret material shall be transmitted under a continuous chain of signed receipts.

2. Secret material shall be covered by a receipt between units and other authorized addressees and between custodians within the same unit.

3. Receipts for Confidential material are not required.

4. Receipts shall be provided by the transferring unit and the forms shall be attached or enclosed in the inner envelope or cover. Postcard receipt form, CG-9733 "document Receipt" may be used for this purpose.

   a. Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

   b. A duplicate copy of the receipt shall be retained in a suspense file until the signed original is returned. If a signed receipt is not received within 45 days, follow-up action shall be initiated. The cognizant Area/District security manager shall be informed. If after the follow-up action, a signed receipt is not returned or the addressee indicates non-receipt, an incident involving classified material shall be submitted in accordance with chapter 12 of this manual.

   c. Copies of signed receipts shall be retained for a period of 4 years.

J. **HANDCARRYING CLASSIFIED MATERIAL.** Individuals handcarrying classified material, either within or outside of a unit, must take every precaution to prevent unauthorized disclosure of that material.

1. Authorization to handcarry classified material.

   a. Individuals who handcarry classified material shall be briefed on their duties and responsibilities as detailed in this chapter and authorized in writing by the Commanding Officer. A clearance verification letter or message may serve as the written authorization. However, it shall specifically state that the individual is authorized to handcarry classified information for the command. Multiple designations may be listed in the same correspondence. One time authorization letters shall be done for individuals handcarrying classified information in a travel status.

   b. The DOD Courier Authorization Card (DD Form 2501) shall only be issued to personnel who handcarry classified material to, from or through a DOD facility. Issuance of DD 2501 shall be strictly controlled

(1) The DD 2501 does not certify the security clearance of the bearer. Individuals who handcarry classified material must still certify their security clearance to the cognizant organization.

(2) The return address of the issuing Command Security Officer (CSO) shall be typed or stamped on the form.

(3) The expiration date shall not exceed one year.

(4) To prevent unauthorized persons from obtaining blank cards, CSOs shall be responsible for performing or ensuring the performance of the following security and accountability functions:

(a) Establish an accountability system to include a positive method for issue, return, destruction, or expiration of courier cards when no longer authorized for use. The issuing authority shall maintain a record of cards issued for 4 years. Unissued cards shall be inventoried annually and the results maintained for 2 years. Records and inspections of courier cards may be incorporated into an existing accountability system such as Armed Forces Identification Cards.

(b) Cards shall be stored in a locked container of at least 12-gauge steel.

2. Handcarrying Within a Command.

a. For any movement within a unit requiring transportation, classified material shall be prepared for transmittal in accordance with this chapter, Except that a briefcase may suffice for an outer cover.

b. For handcarrying within the same building provide sufficient covering to prevent inadvertent disclosure of the classified information. Classified cover sheets (SF 703 through SF 705) shall be used for this purpose.

c. Classified material shall not be delivered to and left in an office when persons authorized to receive it are not present.

3. Handcarrying in a Travel Status.

a. Because of the security risk inherent in handcarrying classified material while in a travel status, commanding officers shall only authorize handcarrying when:

(1) The classified material is required at the travelers destination;

(2) The classified material is not available at the unit to be visited: and

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

b. The CSO shall be advised when anyone in a travel status needs to handcarry classified material to or from the unit. The CSO shall brief individuals authorized to handcarry or escort classified material about the provisions of this chapter, and ensure that a courier letter is issued.

4. Protection During Handcarrying in a Travel Status. When the handcarrying of classified material while in a travel status is authorized, the following requirements shall be met:

a. The classified material shall be prepared as if it were being sent via USPS first class mail with the address of the travelers parent command as the addressee.

b. The classified material shall be in the physical possession of the individual at all times unless proper storage at a U. S. Government activity or appropriately cleared contractor facility (continental U. S. only) is available. The handcarrying of classified information on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage at a government facility or a cleared contractor facility. When surrendering any package containing classified material for temporary storage, the individual shall obtain a receipt signed by an authorized representative of the government activity or contractor facility, which has accepted responsibility for safeguarding the package.

c. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

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

e. The originating unit shall maintain a signed receipt listing all classified material carried or escorted by individuals. If possible the classified material shall be returned to the originating unit by a more secure method.

If the classified material is to be permanently transferred, a signed receipt shall be returned to the originating command. If not, upon return of the traveler, all classified material shall be inventoried and returned to accountability.

f. If difficulty is encountered in foreign customs inspections, individuals should refuse to disclose the classified material to customs inspections and should insist upon assistance of the local U. S. military or State Department representative at the port of entry or departure.

g. Additional procedures to be followed for persons carrying classified material aboard a U. S. air carrier within the U. S.:

(1) In all instances, the classified documents being carried will be contained in sealed envelopes. Should such envelopes be contained in a briefcase or other carry-on luggage, and the item is opened for inspection by airport security, personnel should be able to inspect the envelope without opening it.

(2) In the event that authorized security personnel challenge the courier, the courier shall inform them that the envelope must remain sealed and present an official U. S. Government ID card and courier authorization letter. If security personnel insist on examining the contents the courier shall not allow such inspection and make no further attempt to board the aircraft.

(3) In rare instances, classified material will be in sealed packages which, due to size, weight, or other physical characteristics, are not suitable for processing as outlined above. Persons carrying such material are subject to the screening process as mentioned above except as follows. Competent authority that has authorized the transport of the classified material shall notify an official of the appropriate air carrier in advance of this situation. Upon arrival at the airport, the courier shall report to the appropriate airline ticket counter prior to boarding, present his or her documentation and description of the classified package to the airline official present. In the event airline personnel question the authenticity of the documentation or identification of the passenger, they should be requested to contact a representative of the authorizing official as shown on the courier letter of authorization for verification. When the airline personnel are satisfied, they should provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container or package from physical or other type inspection. The passenger and other items he or she may be carrying are subject to routine screening. If the airline representative is not satisfied with the authenticity of the

passenger or documentation, no further attempt shall be made to board the plane.

5. Courier Letter. Courier letters are required only when handcarrying classified material in a travel status. This refers to one-time instances where specific classified material is handcarried or escorted via private, public or government conveyance between two designated points. This does not include routine courier duties; such as classified message pick-up, Defense Courier duties, CMS draws, etc. Signed copies of courier letters shall be retained for four years. The courier letter shall:

a. Give the full name of the individual and his/her military unit.

b. Describe the type identification the individual will present.

c. Describe the material being carried (e.g., three sealed packages, 9" x 18" x 24", addressee and addresser).

d. Identify the point of departure, destination, and known transfer points.

e. Show the date of issue and an expiration date.

f. Have a statement that the named individual is an authorized courier for the unit.

g. List the name, title and signature of the official issuing the letter. Each package or carton to be exempted will be signed on its face by the official who signed the letter.

h. List the name and telephone number of the official designated to confirm the letter of authorization. The telephone number shall be an official U. S. government number.

i. Have a statement endorsed by the courier that he or she has been properly briefed and understands his or her duties and responsibilities. This statement shall be retained for a minimum of 4 years; it need not be executed on each occasion that the individual is authorized to transport classified information provided a signed statement is on file.

CHAPTER ELEVEN – DESTRUCTION

A. GENERAL.

1. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information.

2. Classified **record** material may be destroyed only when destruction is the disposition authorized by the Paperwork Management Manual, COMDTINST M5212.12 (series).

3. Units will continuously review their classified holdings. Classified information shall be destroyed when determined to be no longer required for operational or administrative purposes.

4. Additional policy must be followed when destroying Communications Security (COMSEC) material as contained in CMS-1(series) and CMS-21(series).

5. Policy for destruction and handling of material marked For Official Use Only (FOUO) is contained in the Privacy and Freedom of Information Acts Manual, COMDTINST M5260.3 (series).

6. Unclassified material, including formerly classified material which has been declassified, unclassified messages, and FOUO material, does not require the same assurances of complete destruction. To avoid overloading a unit's classified material destruction system; unclassified material should be introduced only when the commanding officer or higher authority determines it to be required because of unusual security considerations or efficiency.

B. APPROVED DESTRUCTION METHODS. Destruction devices must be approved by NSA, as listed in NTISSI 4004 Annex B, NSA Evaluated Destruction Devices. Pulpers, pulverizers, or shredders may be used for the destruction of paper products and some forms of computer media. Only paper-based products may be destroyed by pulping. Classified material in microform, that is, microfilm, microfiche, or similar high data density material may be destroyed by burning or chemical decomposition, or other methods as approved by the cognizant security manager. Equipment approved for the destruction of classified material shall be operated properly and provided with regular maintenance, as suggested by the manufacturer. The following are the approved methods for the destruction of classified material.

1. Burning. When burning is used for destruction of classified information, steps shall be taken to ensure that the wind or draft does not carry portions

of burned material away and that the resulting ash is broken up sufficiently to preclude reconstruction.

2. Shredding. Any crosscut shredder whose residue particle size is equal to or smaller than 1/32 of an inch in width by ½ inch in length is approved for the destruction of all classified paper material, magnetic tape, card and flexible diskette (floppy disk). Shredders shall not be used to destroy classified microfilm, microfiche or similar high information density human readable material.

3. Pulping (Wet Process). Wet process pulpers with a ¼ inch or smaller security screen may be used to destroy classified water-soluble material. Since pulpers only destroy paper products, staples, paper clips and other fasteners shall be removed to prevent clogging the security screen.

4. Pulverizing (Dry Process). Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use, unless installed in a noise and dust proof enclosure. Some pulverizers and disintegrators may be used to destroy photographs, film, typewriter ribbons, magnetic tape, flexible diskette (floppy disk), and glass slides and offset printing plates. Pulverizers and disintegrators shall have a 3/32-inch or smaller security screen.

5. Chemical. Classified microfilm or microfiche may be destroyed by chemical process. For example, in an acetone bath.

6. Destruction of Classified Equipment. All components of classified equipment shall be destroyed by any method that destroys them beyond recognition.

7. Eradication of Magnetic Media. Destruction of classified Automated Information System (AIS) magnetic media shall be in accordance with the Automated Information Systems (AIS) Security Manual, COMDTINST M5500.13 (series). All other types of classified magnetic media other than that containing CMS and Sensitive Compartmented Information (SCI) material may be declassified using approved degaussing equipment. Magnetic media may be handled on an unclassified basis and the classified information may be considered as being destroyed provided that:

   a. All markings identifying previous source, subject matter, use or classification of the information previously recorded are removed from the media;

   b. The manufacturers instructions for operating the degaussing equipment are complied with; and

c. The destruction records, as required, are executed upon eradication of the classified information.

C. <u>DESTRUCTION PROCEDURES</u>.

1. Classified material shall only be destroyed by authorized means by individuals cleared to the level of the material being destroyed. Two individuals shall be responsible for destroying Top Secret and Secret material. These individuals must have personal knowledge of the actual material destroyed.

2. When Top Secret and Secret material is placed in a "burn bag" for central destruction, the witnessing officials shall sign the record when the material is actually placed in the burn bag. When the burn bags are destroyed, appropriately cleared personnel must witness the destruction. The persons accomplishing the actual destruction need not sign the record of destruction. A signature for the number of bags destroyed, however, would be appropriate.

3. The personnel tasked with the destruction or preparation for destruction of classified material shall be thoroughly familiar with the requirements and procedures for safeguarding classified information. They shall be thoroughly briefed on the following:

   a. Safeguarding all classified material entrusted to them for destruction.

   b. Conducting a thorough page check prior to destruction.

   c. Observing all documents destroyed or being prepared for destruction and checking the residue of locally destroyed material to ensure that destruction is complete and reconstruction is impossible.

   d. Taking precautions to prevent classified material or burning portions of classified material from being carried away by wind or draft.

   e. Completing and signing all appropriate records of destruction.

D. <u>CLASSIFIED WASTE</u>. Classified waste shall be destroyed as soon as practicable. Containers used for the accumulation of Secret classified waste shall be dated when the first item of classified waste is deposited. If, after 30 days, the classified waste has not been destroyed, it shall be entered into the accountability records of the Security Control Point (SCP). It is not necessary to identify the individual items of classified waste when entering the waste into accountability.

It is sufficient to identify simply as one container, box and bag etc., Secret classified waste. When destruction is completed, a record of destruction will be prepared.

E. EMERGENCY DESTRUCTION.

1. Units located outside the 50 United States and all deployable units shall include in their Emergency Action Plan (EAP) a "Destruction Bill" for the disposition of classified information during an emergency. The following factors shall be considered when developing or evaluating a units destruction bill:

   a. Level of sensitivity of classified material held by the unit.

   b. Proximity of land-based units to hostile or potentially hostile forces.

   c. Flight schedules or ship deployments in the proximity of hostile or potentially hostile forces.

   d. Size and armament of land-based units and ships.

   e. Sensitivity of operational assignment. (Contingency planning should also be considered).

   f. Potential for aggressive action of hostile forces.

2. In emergency destruction planning, the following measures shall be taken:

   a. Reduction of the amount of classified material held by a unit as the initial step toward planning for emergency destruction.

   b. Storage of less frequently used classified material at more secure units in the same geographical area (if available).

   c. Emphasis on the priorities for destruction, designation of personnel responsible for destruction, and the designation of places and methods of destruction. If any destruction site or any particular piece of destruction equipment is to be used by more than one activity or entity, the order or priority for use of the site or equipment must be clearly delineated.

   d. Authorization for the senior individual present in an assigned space containing classified material to deviate from established plans if circumstances warrant.

e. Emphasis on the importance of beginning destruction sufficiently early to preclude loss of material. The effect of premature destruction is considered inconsequential when measured against the possibility of compromise.

3. Drills shall be conducted and documented semiannually to ensure that those responsible are familiar with the implementation of the EAP. The drills shall be used to evaluate the effectiveness of the plan and the resources required to carry it out. At no time shall actual classified material be used in the conduct of EAP drills.

4. For units holding COMSEC material, additional emergency destruction policy and guidance is contained in CMS-1 (series) and CMS-21 (series).

F. PRIORITY FOR EMERGENCY DESTRUCTION.

1. The destruction bill shall require that classified information be assigned a priority for destruction. These priorities shall be based on classification level in descending order (Top Secret, Secret, Confidential). In order to accomplish this, classified information shall be segregated by priority within the security container.

2. In addition to the use of routine classified material destruction equipment, the following methods shall be considered:

a. Classified material may be jettisoned or sunk in an emergency under the following conditions:

(1) COMSEC material. Refer to CMS –1(series) and CMS-21 (series) for criteria for jettisoning and sinking COMSEC material.

(2) Other Material. Classified material may be jettisoned at sea to depths of 1000 fathoms or more. If that water depth is not available, and if time does not permit other means of emergency destruction, the material shall, none-the-less, be jettisoned to prevent its easy capture. When shipboard emergency plans include jettisoning, weighted bags shall be available. If a vessel is to be sunk through intentional scuttling or is sinking due to hostile action, classified material shall be locked in security containers and allowed to sink with the vessel rather than attempting jettisoning.

b. Dismantling or smashing metallic items, beyond reconstruction, by available means such as sledgehammers, cutting tools, torches, etc.

c. Use of disposal equipment not normally associated with the destruction of classified material, such as garbage grinders, sewage treatment plants and boilers.

d. As a last resort, and where none of the methods previously mentioned can be employed, consideration should be given to dousing the classified material with a flammable liquid and igniting it, as an alternative to its certain loss.

G. REPORTING EMERGENCY DESTRUCTION. Accurate information concerning the extent of emergency destruction of classified material is second in importance only to the destruction of the material itself. Accordingly, the facts surrounding the destruction shall be reported to the cognizant security manager, Commandant (G-CFI) and other interested units by the most expeditious means. Reports shall contain:

1. Material destroyed

2. Classification of material

3. Date of destruction

4. Method of destruction

5. Listing of any material not destroyed and feared compromised/captured

CHAPTER TWELVE – COMPROMISES, ADMINISTRATIVE DISCREPANCIES, WAIVERS & EXCEPTIONS

A. INTRODUCTION. The policies and procedures in this and related security directives are intended to prevent the compromise of classified information. The handling or dissemination of classified information contrary to the provisions of these directives could result in a compromise or possible compromise of the information. Whereas an infraction of a specific requirement may not subject information to compromise in one instance, an infraction of the same rule under different circumstances could result in a compromise. For this reason, all violations of the regulations in this manual shall be reported and corrective action taken.

B. COMPROMISE.

1. A compromise is the disclosure of classified information to a person who is not authorized access to that information. The unauthorized disclosure may have occurred unknowingly, willfully or through negligence. Compromise is confirmed when conclusive evidence exists that classified information has been disclosed to an unauthorized person.

2. A possible compromise occurs when some evidence exists that classified information has been subjected to unauthorized disclosure, loss, or when considering the location and length of time classified information was not properly stored or controlled, it may have been exposed to a person not authorized for access.

3. The compromise of classified information presents a threat to national security. The seriousness of the threat must be determined and measures taken to negate or minimize the adverse effect of the compromise. For this reason, a uniform method of reporting and investigating possible compromises and administrative discrepancies has been established.

C. ADMINISTRATIVE DISCREPANCY. Failure to follow established security related procedures, which do not subject classified material to compromise or possible compromise.

D. INITIAL REPORTING AND RESPONSIBILITIES.

1. Any civilian employee, military personnel, or other person associated with the Coast Guard, having knowledge of the loss, unauthorized disclosure, or possible compromise of classified information, or of an infraction of security regulations shall immediately advise his/her command security officer. Once advised of the incident, commands shall report or assure that the matter is reported immediately in accordance with the procedures set forth in this manual.

2. Compromise or Possible Compromise. When classified material has been lost or compromised, actions shall be initiated by the command security officer to accomplish the following objectives:

   a. Regain custody of the material, if feasible, and afford it proper protection. If it is not feasible to regain custody of material believed to be in an area beyond the jurisdiction of the U. S., any information identifying the location of the material shall be classified at the same level as the unretrieved material.

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

   c. Discover the weakness in security procedures, which caused or permitted the compromise or potential for compromise, and revise procedures as necessary to prevent recurrence.

   d. Submit a report of the incident in accordance with established procedures as detailed in this directive.

   e. If individual responsibility is established, report in accordance with the Military Personnel Security Program, COMDTINST M5520.12(series), and take appropriate administrative/disciplinary action.

3. Administrative Discrepancy.

   a. A discrepancy in administrative procedures that does not subject material to compromise is considered an administrative discrepancy. When an administrative discrepancy is discovered, submit a report of the incident in accordance with established procedures as detailed in this directive.

   b. The CG-4764, Administrative Discrepancy Notice, is cancelled and no longer authorized for use.

4. Report of incident involving classified material.

   a. A report of incident involving classified material is an immediate notification and presentation of the facts for the purpose of limiting and assessing the damage to the national security. Reports shall be made to the CSO of the discovering unit who will submit a formal message report (see exhibit 4-1) within two working days. The intent is to notify all cognizant officials as soon as possible to limit further damage, assess weaknesses and correct a discrepancy if appropriate. If formal message reporting cannot be accomplished in two days, the cognizant security manager will be notified telephonically.

b. Reports of incidents involving classified information shall contain the following information:

(1) Type of report:

(a) Compromise; or

(b) Possible Compromise; or

(c) Administrative Discrepancy

(2) Type of incident:

(a) Compromise or Possible compromise;

1. Improper Destruction; or

2. Unauthorized access; or

3. Improper transmission (transmission via non-secure means or use of unauthorized equipment); or

4. Improper storage; or

5. Loss of material; or

6. Found material (material not in accountability system or previously reported as lost) not subjected to possible compromise; or

7. Other (explain)

(b) Administrative Discrepancy;

1. Mailed via non-registered/certified mail; or

2. Sent in single container; or

3. Markings on outer container divulged classification of contents; or

4. Classification not marked on inner container; or

5. No return receipt; or

6. Inadequate wrapping: not securely wrapped or protected; or

7. Received in poor condition: compromise improbable; or

8. Addressed improperly; or

9. Classified by unauthorized original classifier; or

10. Markings incorrect; or

11. Classified by, reason for classification, or declassify on, incorrect or missing (originally classified documents); or

12. Derived from or declassify on line incorrect or missing (derivatively classified documents); or

13. Other (explain)

(3) Complete identification of all material involved including;

(a) Unclassified title

(b) Classification

(c) Originator

(4) Identity of all personnel involved including;

(a) Full name

(b) SSN

(c) Security Clearance

(d) Basis of Security Clearance

(5) A statement of actions taken upon discovery of incident and description of events.

(6) Weakness leading to the incident

(7) Corrective actions taken and actions taken to preclude recurrence

(8) Disciplinary action taken, if any

(9) Unit incident number, to include;

(a) Fiscal year

(b) Sequential number

5. Incident reports shall be sent for action to the cognizant security manager with an information copy to the following:

a. Commandant (G-CFI)

b. The unit having custodial responsibility if other than the originator of the incident report

c. The unit responsible (if administrative discrepancy)

d. Telecommunicatons and Information Systems Command (TISCOM) (for incidents involving NATO or COMTAC information)

e. Commandant (G-CIM-1) (for incidents involving compromise through use of information systems)

6. Incidents involving district staffs and area staffs shall be sent for action to Commandant (G-CFI).

7. After reviewing the incident, the cognizant security manager shall respond to the unit with a classified material incident response message. A classified material incident response message shall contain:

a. Security manager's determination on possibility of compromise and determination of necessity to inform the originator of the material. (If originator will be notified, a request for assessment of possible damage to national security will be requested).

b. Concurrence or non-concurrence on actions taken upon discovery and to preclude recurrence.

c. General comments (may include authority to remove material from accountability or request further information).

d. Incident closure or further investigation required.

e. Area/District incident number (to include fiscal year and sequential number).

E. SECURITY INVESTIGATIONS. A security investigation is a preliminary inquiry conducted by a Coast Guard security manager or security specialist with the proper credentials. The inquiry is to determine what type of additional investigation, if any, should be conducted as a result of a incident involving classified information, problems encountered during an evaluation or other instances deemed appropriate in the interest of national security. At the conclusion of the security investigation, the security official shall:

1. Recommend an administrative or criminal investigation be conducted, or when satisfied that no benefit would be derived from further investigation, close the investigation.

2. Provide a written report to his/her chain of command with an information copy to Commandant (G-CFI).

3. Should circumstances warrant further investigation, the security official shall submit a report to the commanding officer of the command with a copy to Commandant (G-CFI). The report shall state the facts of the case and the basis for their recommendation for an additional investigation.

F. ADMINISTRATIVE INVESTIGATIONS.

1. When an incident report cannot effectively assess a possible compromise, an administrative investigation may be directed by the cognizant security manager or Commandant (G-CFI) in accordance with the Administrative Investigations Manual (AIM), COMDTINST M5830.1 (series). It is Coast Guard policy that the least extensive type of investigation, which will meet the needs of the situation, shall be utilized. Refer to the AIM for a description of the different types of administrative investigations and for guidance in selecting the investigation appropriate to the circumstances. When in doubt, the servicing legal officer may be consulted for guidance.

2. After endorsement by the Convening Authority, administrative investigations shall be routed through reviewing authorities, including the cognizant security manager, to Commandant (G-LGL).

3. Reports of investigation shall be carefully examined by each reviewing authority that shall take the following actions:

   a. Return by endorsement any deficient report for additional investigation or corrective action

   b. Evaluate the corrective measures taken to preclude recurrence.

c. Determine whether security practices have been corrected. When appropriate, submit recommendations for changes to security requirements to Commandant (G-CFI).

d. Forward the reports by endorsement, setting forth appropriate comments and recording approval or disapproval in whole or in part, of the proceedings and findings of fact.

e. Reviewers shall ensure that copies of their endorsements are forwarded to previous reviewers and to the units which have received a copy of the report of investigation.

G. INVESTIGATION ASSISTANCE. Commanding Officers may request assistance from the Coast Guard Investigative Service (G-O-CGIS) in incidents involving classified material which are beyond the unit's capabilities or resources, and which fall within the functions and responsibilities of CGIS in accordance with the Investigative Assistance Manual, COMDTINST M5520.5(series).

H. INCIDENTS INVOLVING SPECIAL TYPES OF INFORMATION.

1. Communication Security (COMSEC) Information. CMS-1, Communications Security Material System, describes reportable COMSEC insecurities. Information copies of COMSEC insecurities shall be provided to the cognizant security manager and Commandant (G-CFI).

2. Sensitive Compartmented Information (SCI). Commandant (G-OCI) is the Coast Guard Special Security Officer (SSO). As such, Commandant (G-OCI) is the Coast Guard point of contact for SCI matters. Incidents involving SCI shall be reported as soon as possible to the responsible SSO. The SSO will then direct further action.

I. COMPROMISE THROUGH PUBLIC MEDIA. When an individual becomes aware that classified information has been compromised as a result of disclosure in a newspaper, magazine, book, pamphlet, internet web page, radio or television broadcast, or other means of public dissemination, a prompt report shall be made to Commandant (G-CFI) via the cognizant security manager. The report shall fully identify the information, the media concerned, the reporter or author involved and the report shall cite those portions alleged to reveal classified information. Such reports shall be classified, commensurate with the level of the classified information involved in the compromise. If possible, determine who classified the information appearing in the media.

J. DEBRIEFINGS IN CASE OF UNAUTHORIZED ACCESS.

1. In cases where a person has had unauthorized access to classified information, the CSO will debrief the individual as follows:

a. If the unauthorized access was by a person with the appropriate security clearance but no need-to-know, debriefing is usually appropriate only so far as necessary to ensure that the individual is aware that the information to which they had unauthorized access is classified and requires protection.

b. If the unauthorized access by and individual without the appropriate security clearance, the individual should be advised in writing of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if they fail to do so. This can be accomplished by executing a non-disclosure agreement (SF-312).

c. In any case where the person to be debriefed may be the subject of criminal prosecution or disciplinary action, consult with legal counsel before attempting to debrief the individual.

d. In all cases, the person being debriefed will have a properly executed non-disclosure agreement (SF-312) on file.

K. <u>WAIVERS AND EXCEPTIONS</u>. For the purposes of this manual, a waiver is defined as temporary exemption to policy requirements, and an exception is a permanent exemption to policy requirements. Waivers and exceptions to the requirements of this manual will be considered on a case by case bases. This section does not apply to waivers and exceptions from COMSEC requirements. Coast Guard Telecommunications and Information Systems Command (OPS-4) handle such requests.

1. Blanket waivers and exceptions from security requirements are not authorized. Requests for waivers and exceptions shall be considered on an individual basis.

2. Requests for waivers shall be sent in writing to the cognizant security manager for action. Action shall be taken within 60 days. The cognizant security manager shall forward a copy of all correspondence pertaining to approved requests to Commandant (G-CFI). The cognizant security manager will numerically identify each waiver as follows:

a. The first 2 digits represent the area or district of the unit initiating the request.

b. The next 4 digits will be the Standard Subject Identification Code (SSIC) of the request.

c. The next digit represents “W” for waiver.

d. The next 2 digits represent the serial number (sequentially), beginning annually on 1 January with 01.

e. The last 2 digits represent the calendar year.

f. Examples: D1-5510-W-01-98
LANT-5510-W-01-98

3. Requests for waiver extensions or for exceptions shall be sent in writing via the cognizant security manager to Commandant (G-CFI) for action.

4. Waivers shall be granted for a period of 1 year or less. Waivers may be extended by Commandant (G-CFI) beyond 1 year only after a review of the circumstances described in the request for the extension. These requests shall be submitted to the cognizant security manager no later than 60 days prior to the expiration date. Each extension request shall identify any previous extensions granted for the same item.

5. Requests for waivers and exceptions shall identify compensatory security measures currently in effect or planned.

6. Deficiencies which units can correct within 60 days will not require waivers; however, compensatory security measures shall be taken until the correction is made.

7. The cognizant security manager shall be notified in writing whenever a deficiency for which a waiver has been granted is corrected.

8. Exceptions shall be granted only when correction of a deficiency is not feasible or when the security being provided is equivalent to or better than that required by this manual. Requests for exceptions shall cite better or equivalent protection being provided or explain why it is not feasible.

9. Requests for waivers and exceptions shall be thoroughly reviewed before forwarding to the cognizant security manager to ensure that all avenues for compliance have been exhausted. The approval of specific waivers and exceptions does not relieve commanding officers of the responsibility for maintaining security per all other provisions of this manual.

10. Each waiver or exception request shall be identified by the subject, the name of the unit initiating the request, the date, and shall include the following:

a. Statement of the waiver or exception requirement and reference to the specific paragraph in this manual that cites the standards that cannot be met.

b. Specific description of the conditions that caused the need for the waiver or exception and reasons why the standards in this manual cannot be met.

c. Measures that are in effect to compensate for noncompliance with required standards of protection.

d. Actions initiated or planned to eliminate the deficient condition(s) and estimated time of completion.

e. Resources e.g., cost, manpower, required to eliminate the deficient condition(s).

f. Impact on mission and any problem(s) that will interfere with operating requirements.

Exhibit 4-1

EXAMPLE OF AN INCIDENT INVOLVING CLASSIFIED MATERIAL REPORT

P (DATE TIME GROUP)

FM (UNIT DISCOVERING INCIDENT)

TO (COGNIZANT SECURITY MANAGER)

INFO COMDT COGARD WASHINGTON DC//G-CFI//

UNIT HAVING CUSTODIAL RESPONSIBILITY (IF NOT ORIGINATOR)

UNIT RESPONSIBLE (IF ADMIN DISCREPANCY)

COGARD TISCOM ALEXANDRIA VA//OPS-4// (IF NATO OR COMTAC)

COMDT COGARD WASHINGTON DC//G-CIM-1// (IF INCIDENT INVOLVES COMPROMISE THROUGH USE OF INFORMATION SYSTEM)

BT

UNCLAS FOUO (CLASSIFY ONLY IF APPROPRIATE) //N05510//

SUBJ: INCIDENT INVOLVING CLASSIFIED MATERIAL

A. CLASSIFIED INFORMATION MANAGEMENT PROGRAM, COMDTINST M5510.23

1. TYPE OF REPORT: (SEE PARAGRAPH 12-D-4-b- (1))

2. TYPE OF INCIDENT: (SEE PARAGRAPH12- D-4-b-(2))

3. MATERIAL INVOLVED: (SEE PARAGRAPH 12-D-4-b-(3))

4. PERSONNEL INVOLVED: (SEE PARAGRAPH 12-D-4-b-(4))

5. ACTIONS TAKEN UPON DISCOVERY OF INCIDENT AND DESCRIPTION OF EVENTS:

6. WEAKNESS LEADING TO INCIDENT:

7. CORRECTIVE ACTIONS TAKEN AND ACTIONS TAKEN TO PRECLUDE RECURRENCE:

8. DISCIPLINARY ACTION TAKEN:

9. UNIT INCIDENT NUMBER: (SEE PARAGRAPH 12-D-3-b-(9))

BT

CHAPTER THIRTEEN – SPECIAL CATEGORIES OF INFORMATION

A. **GENERAL.** The Coast Guard may become involved with special categories of information established by other government agencies. In this respect, the Coast Guard shall respect and comply with the special requirements imposed by cognizant authorities with regard to access, distribution and protection of unique types of information.

B. **SPECIAL ACCESS PROGRAM (SAP).**

1. Normally, security requirements for Confidential, Secret or Top Secret information provide sufficient safeguarding. Any program requiring additional security protection and handling measures, special investigative, adjudicative and clearance procedures, or special briefings, reporting procedures or formal access lists is considered a SAP.

2. The Coast Guard does not have the authority to establish a SAP but Coast Guard personnel may become involved with SAPs established by other government agencies. Participation by Coast Guard personnel in SAPs established by other government agencies shall be reported in writing, to the OST Director, Office of Security (M-70) via Commandant (G-OCI).

C. **SENSITIVE COMPARTMENTED INFORMATION (SCI).** SCI is highly sensitive national security information to which access is based on a strict NEED-TO-KNOW basis. The SCI system is a national intelligence community security program promulgated by the Director of Central Intelligence (DCI). The Office of Naval Intelligence (ONI) administers the program to the U. S. Coast Guard through the U. S. Navy. A Special Security Officer (SSO) is assigned and designated in writing by the Assistant Commandant for Operations (G-O) as the Coast Guard point of contact for SCI matters. Commandant (G-OCI) is the U. S. Coast Guard SSO and is the program manager for all SCI matters. The SSO is charged with ensuring SCI security regulations are maintained and enforced. A Sensitive Compartmented Information Facility (SCIF) is established where there is a need to receive, store and discuss SCI. Each SCIF will have an SSO assigned.

D. **RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD).**

1. Atomic Energy Act. Nothing in this manual shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended or to the regulations of the Department of Energy (DOE) under that act. RD and FRD shall be handled, protected, classified,

downgraded and declassified in accordance with the provisions of the Atomic Energy Act and the regulations pursuant to it.

2. Custody and Storage.

   a. In order to have access to RD, Coast Guard personnel must possess a valid DOE clearance. Information concerning DOE clearances is contained in the Military Personnel Security Program, COMDTINST M5520.12 (series).

   b. It is recommended that RD documents be maintained in a separate approved storage container. If a separate container is not available these documents shall be maintained in a separate drawer of an approved security container holding other classified information. RD shall not be intermingled with other classified material.

   c. FRD is protected as national security information and does not require special clearances or handling practices by entities located on U. S. Government property; however, dissemination to foreign governments or organizations is strictly controlled by DOE.

   d. Documents containing RD and FRD remain the property of DOE. Accordingly, DOE may cause inspections to be made of the security measures in effect within each Coast Guard unit having custody of RD and FRD.

3. Transmission. RD and FRD shall be transmitted in the same manner as other material of the same security classification with the following precautions:

   a. Units shall ensure that RD and FRD are clearly marked as such on the inner transmission container.

   b. When envelopes containing RD are received in any office or at any unit, they will be delivered unopened to the Restricted Data Control Officer or the next senior person holding a valid DOE clearance at the appropriate level.

   c. Should RD or FRD be inadvertently received by a unit with no appropriately cleared personnel, the material shall be returned unopened to the originator with a brief letter of explanation. A copy of the letter shall be forwarded to Commandant (G-CFI). Refer to chapter 12 for guidance pertaining to incidents involving classified material.

   d. Messages containing RD must be off-line encrypted.

CHAPTER FOURTEEN - OPERATIONS SECURITY (OPSEC)

A. INTRODUCTION.

1. In 1987, then President Ronald Reagan signed National Security Decision Directive (NSDD) 298. This directive mandates that all executive agencies develop and maintain an OPSEC program.

2. OPSEC is defined as a systematic and analytical process by which the U. S. Government and its supporting contractors can deny potential adversaries, information about capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

3. This information about our intentions, capabilities, or activities is known as critical information. Compromise of this critical information may allow an adversary to gain a significant military, law enforcement, economic, political or technological advantage. That advantage becomes significant if it prevents the Coast Guard from effectively completing its assigned missions.

4. Coast Guard units have been and continue to be monitored by groups and organizations involved in illicit activity. Narco-traffickers and alien smuggling organizations as well as fishermen are known to use a variety of methods to obtain information about our operational units. Extensive documented evidence exists that details the lengths these groups have gone to, to track, monitor, and observe our activities. The only way for the Coast Guard to be successful in completing its assigned military and law enforcement operations is through the employment of OPSEC. Organizationally, we must protect information such as asset movement, capabilities and intentions. This involves all personnel, active, reserve, auxiliary and civilians at every command. A concerted effort must be taken to ensure <u>everyone</u> is aware that the threat is real and active in all areas of our law enforcement operations.

5. A unique aspect of OPSEC is that you must step out of your normal frame of reference and take the adversary's perspective. You must "put on your bad guy/girl's hat" and think; "If I were going to smuggle drugs, people or fish illegally, this is how I would do it and avoid the Coast Guard."

B. APPLICATION.

1. The OPSEC process consists of five inter-related steps. This process is designed to step the user through a methodical series of actions to arrive at a conclusion. The conclusion may be that nothing can be done to protect an activity, while at other times it will provide the most appropriate response to a vulnerability and threat. The five steps and a brief description of each follows.

a. Identify Critical Information - Determine what information is available to one or more adversaries that would harm the organization or the unit's ability to effectively carry out a particular operation. This critical information constitutes the few pieces of information that are central to the mission's success. Critical information is often classified when pertaining to national security issues such as military or intelligence operations. Many law enforcement missions the Coast Guard performs do not meet these criteria and are considered unclassified but sensitive. The unclassified operations are where the greatest emphasis needs to be, as these operations constitute the majority of our missions.

b. Identify your Threat - Knowing who the adversaries are, and what information they require to meet their objective is essential in determining what information is truly critical. In any given situation, there is likely to be more than one adversary and each may be interested in different types of information. The adversaries' ability to collect, process, analyze, and utilize information must also be considered. In other words, do they have the **capability and intention** to make them a credible threat? If either element is missing, the threat is not there. For example, a group that desires information contained in encrypted radio transmissions, but does not have the *capability* to obtain it is not a threat, while a group that desires to know when a cutter or aircraft departs it's unit, and can observe it, is. The objective is to know as much as possible about each adversary and the strategies available to them for targeting the unit and operation. It is especially important to tailor the adversarial threat to the actual operation and, to the extent possible, determine what the adversaries' capabilities are for the specific time and place the operation will be conducted.

c. Identify your Vulnerabilities - Determining vulnerabilities involves analysis of how the operation is usually conducted. The operation must be viewed as the adversary would view it, thereby providing the basis for understanding how the organization really operates. These are the true, rather than the hypothetical, vulnerabilities. The chronology of all events, the timing of actions, and the flow of information and materials must be reviewed. Actions that can be observed, or data that can be intercepted and interpreted or pieced together to derive critical information must be identified. These are the "indicators". An assessment should be made of how vulnerable one's unit is to the adversary seeking any indicators that can provide critical information. Often the newest members of the crew can be the most objective in identifying this information. Exhibit 14-1 provides as list of potential indicators.

d. Risk Assessment**.** What is Risk Assessment? According to the CIA's model, it is "the process of evaluating ***threats to*** and ***vulnerabilities of*** an

asset to give an expert opinion on the probability of loss or damage, and its ***impact***, as a guide to taking action." In order to have risk, you must have three conditions present, an asset (information or property), one or more vulnerabilities and a threat. The absence of any of the three elements removes the risk. Vulnerabilities and threats must be matched. Where a unit's vulnerabilities are exploitable and capabilities and intentions are present, the risk of adversarial exploitation must be expected. Therefore, a high priority for protection needs to be assigned and countermeasures applied. Conversely, where the vulnerability is moderate or slight and the adversary has a limited collection capability, the priority should be medium or low.

e. Apply Countermeasures. Appropriate cost-effective countermeasures to mitigate or control vulnerabilities, threats, or utility of the information to adversaries should be developed. They must be designed to defeat or delay adversarial actions. Countermeasures may include procedural changes, suppression of indicators to deny critical information, deception, perception management, intelligence countermeasures, traditional security measures, or any other action that is likely to work in a given situation. There are no right, wrong, or standard solutions for all situations. This dynamic process requires continual evaluation and creativity. Perhaps the most cost-effective measure a unit can take is to adopt an active and continuing training and awareness program. Clear guidance from the command regarding what can and cannot be talked about outside the confines of the unit can also go a long way. Some countermeasures, by their nature may only be useful once or twice, while others are effective on a long-term basis. The Commanding Officer must then determine which countermeasures are appropriate and cost-effective based on the results of the risk assessment. Exhibit 14-2 provides as list of potential countermeasures.

C. Responsibilities.

1. Commandant (G-CFI) is the OPSEC Program Manager and the Coast Guard OPSEC Officer is assigned from his/her staff. Each Area and District shall have an OPSEC Officer designated in writing.

2. Each Area and District shall provide written OPSEC guidance to all subordinate units.

3. Each Operational Commander must institute all reasonable OPSEC countermeasures. To reach a decision, the Commander must balance the cost of the countermeasure against the cost of revealing the critical information. This decision can only be based after a careful review of the threat. The use of field level reporting has proven instrumental in achieving and maintaining a constant flow of raw intelligence information. This information may also be obtained from the District and Area intelligence staff.

D. **OPSEC Surveys.** An OPSEC survey is a thorough examination of a unit or an operation to determine exploitable vulnerabilities of critical information and to recommend countermeasures. This includes collecting information, making observations and interviewing of personnel. A unit through their cognizant district/area OPSEC Officer or Security Manager can request OPSEC surveys. OPSEC surveys will be coordinated through commandant (G-CFI). Units should expect to commit personnel and associated costs for the period of the survey (two weeks). When an OPSEC survey is completed, a report will be prepared for the requesting unit and will not be distributed without the specific permission of that unit. Lessons learned are encouraged to be shared.

EXHIBIT 14-1

INDICATOR TABLES

Table 1 Common Indicators

a. Indicators Establishing Profiles

1. Access Lists
2. Availability
3. Conferences and meetings
4. Coordination between agencies
5. Readiness
6. Checklist procedures
7. Data processing requirements
8. Fixed sequences of action
9. Hours of operation
10. Identifiers
    - (a)Abbreviation/acronyms
    - (b) Codewords
    - (c) Mission designators
    - (d) Nicknames
    - (e) Project numbers
11. Implementing/executing procedures
12. Inspection/evaluation/test results
13. Interagency/international agreements
14. Capability limiting factors
15. Location of units/resources
16. Mission assigned
17. Weapons procedures
18. Orders
19. Performance criteria
20. Personnel assigned/staff composition
21. Proficiency
22. Quality control
23. Reports/reporting
24. Requirements
25. Restrictions
26. Security checks and tests
27. Security clearance and requirements
28. Signatures features (activities/material)
29. Spontaneous reaction and timing
30. Standard (fixed) operating procedures

31. State of readiness

b. Indicators Showing Deviations

1. Augmentation
2. Backup resources/procedures
3. Convening special groups/staffs
4. Critical timing
5. Deficiencies/breakdowns
6. Distinguishing emblems or logos
7. Efficiency measures
8. Emergency procedures
9. Exercise/rehearsals
10. Homemade codes
11. intensity of activity
12. Key words
    (a) Critical
    (b) Higher headquarters
    (c) Priority
    (d) Rush
    (e) Special
13. Locations
    (a) Origins/destinations
    (b) Pre-positioning assets
    (c) Units/resources
14. Planning conferences
15. Priorities assigned
16. priorities of service
17. Reorganization
18. Requirements change
19. Rush requirements
20. Security awareness and alertness
21. Security clearance Requirements
22. Security enhancements
23. Shortage and limitations
24. Special requirements
25. Times/dates
    (a) Arrival/departure
    (b) Milestones
    (c) Suspense
    (d) Timeliness
26. Volume of service requested/provided

Table 2 Planning Activity

a. Indicators Establishing Profiles

1. Climatology
2. Command Control procedure
3. Conferences
4. Exercising
5. Fighting planning
    (a) Foreign overflight arrangements
    (b) ICAO/FAA flight filing/coordination
    (c) Restricted airspace/ocean areas
6. Force
    (a) Composition
    (b) Disposition
    (c) Pre-positioning
7. Intelligence
    (a) Dissemination
    (b) Source/methods
    (c) Gaps
    (d) Requirements
8. Maps and charts coverage
9. Mission designators
10. Number of aircraft/ships/vehicles
11. Physical Security
12. Planned activity profile
13. Recreation times/sequences
14. Reconnaissance activities
15. Scenarios
16. Search and rescue capabilities
17. Security classification guides
18. Sensor capabilities
19. Spontaneous reaction
    (a) Actions taken without communications
    (b) Action taken without coordination
20. Strategy
21. Tactics
22. Testing
23. Threat assumptions/intelligence

b. Indicators Showing Deviation

1. Actions taken without coordination/communication
2. Force augmentation
3. Pre-positioned forces/material/munitions/fuels

4. Rehearsals
5. Scheduled modification
6. Security augmentation
7. Unit activation
8. Weather limiting factors

Table 3 Administration Activity

a. Indicators Establishing Profiles

1. Accountability records
2. Administrative organization
3. Clerical workload
4. Distribution/address list
5. Document receipt
6. Job and position description
7. Mail volume
8. Mission statement
9. Operational organization
10. Operation plan/order number of nicknames
11. Property/inventory receipts
12. Publication volume/priorities
13. Security classification
14. Security classification guides

b. Indicators Showing Deviations

1. Accidents/incidents/mishaps reports
2. Administrative correspondence
3. Forms requests
4. Mail address changes
5. Mail forwarding
6. Reports distribution
7. Security clearance requests
8. Security investigations
9. Work orders/job requests

Table 4 Civil Government and Commercial Support

a. Indicators Establishing Profiles

1. Facility use
2. Security OPSEC contract specification
3. Contract specifications
4. Memorandums of Agreement
5. Technical studies and reports

6. Trash disposal

b. Indicators Showing Deviation

1. Commercial assistance requirement
2. Commercial personnel movement
3. Commercial manpower
4. Commercial movement of material
5. Courier service
6. Delivery/pickup locations and dates/times
7. Local government notifications
8. Law enforcement coordination/support
9. Requests for proposals/bids
10. Technical representative visits
11. Transportation support
12. Traffic control
13. Vehicle rental
14. Telephone service requests

Table 5 Command and Staff Activity

a. Indicators Establishing Profiles

1. Command control elements
2. Command control procedures
3. Command Control response
4. Commanders/Executive
    (a) Public appearances
    (b) Health
    (c) Leave schedule
    (d) Personnel affairs
    (e) Reaction under stress
    (f) Strategic and technical behavior
5. Commanders/seniors staff member identity
6. Force composition
7. Foreign or interagency liaison personnel
8. Intelligence gaps
9. Inter-command communications/coordination
10. International communication flow
11. Morale and discipline
12. Organizational structure
13. Reaction to hostile actions
    (a) Reaction sequences
    (b) Reaction timing
14. Reconnaissance activity
15. Reconnaissance unit location

16. Staff Officer
    (a) Assignments
    (b) Experience
    (c) Skills and education

b. Indicators showing Deviations

1. Commander/senior staff itinerary
2. Commander's leave schedule
3. Deployment orders
4. Distinguished visitors
5. Force command control
6. intelligence briefing subjects
7. organization restructuring
8. Senior level interests
9. Senior officer schedule
10. Staff augmentation
11. Subject of intelligence emphasis
12. Target damage assessments
13. Unit orders

Table 6 Communication Activity

a. Indicators Establishing Profiles

1. Antenna types/orientation
2. Brevity codes
3. Call signs
4. Circuit system requirements
5. Communication discipline
6. Communication-Electronics operating instructions
7. Communicator signature feature
8. Encryption/encoding/authentication system
    (a) Capabilities
    (b) Circuit where used
    (c) Effective editions/changes dates
    (d) Requirements
9. Flow/volume/intensity
10. Frequencies assigned
11. Automatic identifier (IFF) codes
12. International communications
13. Amateur communication
14. Message delivery efficiency/speed
15. Message format
    (a) Address
    (b) Lengths

(c) Priorities

16. Net/circuit designators
17. Nets/net membership
18. Nodes and choke points
19. Operating restrictions
20. Power requirements/sources
21. Priorities
22. Procedures to counter radio interference action
23. Radio checks
24. Reporting times
25. Security classification
26. Security procedures/authentication procedures
27. System usage
28. Technical studies
29. Telephone usage
30. Transmission signature features

b. Indicators Showing Deviations

1. Authentication requirements
2. Breakdown in communications
3. Hostile radio interference effectiveness
4. Communication degrade
5. Communication electronic procedure modification
6. Communication methods modification
7. Equipment changes/modification
8. Flight safety communication
9. Frequency changes
10. Frequency designators
11. Homemade codes
12. Personal communication
13. Radio silence
14. Rendezvous beacons
15. Routing indicator changes
16. Special capabilities
17. Station changes
18. Telephone service requests
19. Unofficial/personal call signs
20. Weather addresses/priorities

Table 7 Electronic Activity

a. Indicators Establishing Profiles

1. Emissions

2. Altimeter
3. Communications
4. Identification Friend or Foe (IFF)
5. Navigation aids/TACAN beacons
6. Radar
7. Rendezvous beacon

b. Indicators Showing Deviation

1. Electronic Countermeasures
2. Fire control radar
3. Friendly aircraft tracking
4. Search and rescue beacon
5. Target tracking
6. Telemetry transmission
7. Test vehicle tracking
8. Weapons system emission

Table 8 Financial Activity

a. Indicators Establishing a Profile

1. Budget analysis
2. Budget justification statements and summaries
3. Budget projections and estimates
4. Budget requirements
5. Financial plans
6. Operating budgets
7. Temporary duty fund limits
8. Temporary duty funds requirements

b. Indicators Showing Deviation

1. Advance payments
2. Budget supplemental
3. Budget supplemental
4. Programming budget inputs
5. System modifications component funding
6. Temporary duty funding projected
7. Temporary duty fund usage
8. Travel vouchers
9. Unplanned funding actions
10. Year to year comparisons

Table 9 Logistics Support Transportation

a. Indicators Establishing Profiles

1. Cargo/shipment
    (a) Classification
    (b) Identification numbers/codes
    (c) Number of pieces
    (d) Origin/routing/destination
    (e) Priority
    (f) Weight/cubic feet
2. Commercial transport use
3. Courier service
4. Material handling
5. Modes of transport available
6. Movement assembly area
7. Movement node/check points
8. Personal property shipment
9. Requirements
10. Specialized vehicle/aircraft
11. Transportation control numbers
12. Ship/vehicle/aircraft capabilities
    (a) Identification
    (b) Numbers
    (c) Status
    (d) Type
13. Ship/vehicle/aircraft density
14. Ship/vehicle/aircraft movements
15. Ship/vehicle/aircraft schedules

b. Indicators Showing Deviation

1. Container labels
2. Convoy assembly
3. Delivery/pickup suspense dates
4. Munitions movement
5. Name tag
6. Personal Luggage assembly
7. Resource movement
8. Travel authorizations
9. Travel reservations

Table 10 Maintenance and Repair Activity Indicators

a. Indicators Establishing Profiles

1. Aircraft tail numbers

2. Ship hull numbers
3. Ship/vehicle/aircraft density
4. Downtime planned for repair /maintenance
5. Established time to completion of repairs
6. Equipment calibration
7. Equipment design features and nomenclature
8. Equipment nomenclature
9. Maintenance of pre-positioned equipment
10. Maintenance team movement
11. Maintenance activity routine
12. Maintenance trends
13. Material handling
14. Weapons/components procedures
15. Mission/sortie number
16. System/element identification
17. Technical order change
18. Technical studies
19. Test equipment
20. Repair scheduling

b. Indicators Showing Deviations

1. Damage assessment
2. Weapons system modifications
3. Equipment awaiting parts
4. Equipment modifications
5. Failure rates
6. Quality control deficiencies
7. System modification components
8. System-wide maintenance requirements/deficiencies
9. Tool box shortage

Table 11 Material Acquisition and Supply

a. Indicators Establishing Profiles

1. Camouflage
2. Classified stock numbers
3. Water
   (a) Capacity
   (b) Production rate
   (c) Requirements
   (d) Storage capacity
4. Fuels and Lubricants
   (a) Ship/aircraft fuel loads
   (b) Bulk storage records

(c) On hand /inventory
(d) Requirements
(e) Shipment/receipt
(f) Special types
(g) Storage capacity
(h) Supplier/source
(i) Transfer/refueling capacity

5. Maps and Charts
   (a) Availability/coverage
   (b) Production requirement
   (c) Overlays or special details
   (d) Requirements
   (e) Scale
   (f) Short titles/numbers
6. Materials delivery
   (a) Schedules
   (b) Suspense dates/times
   (c) Volumes
7. Material handling
8. Material pipeline nodes and checkpoints
9. Mobility assets
10. Munitions
11. Nameplate data
12. Name tags
13. Parts availability
14. Personal equipment
15. Provisions
16. Provisions requirements/Priorities
17. Quantities on hand/inventory
18. Reliability of parts
19. Requisition
    (a) Priorities
    (b) Procedure
    (c) Timing
    (d) Volume
20. Shelf-life times
21. Stockpile conditions
22. Storage capabilities
23. Survival equipment
24. System modifications components
25. Test equipment

b. Indicators Showing Deviations

1. Equipment awaiting parts
2. Failure rates

3. Munitions movement
4. Pileups
5. Pre-positioned materials, fuels, munitions
6. Repair cycle assets
7. Requisition priorities
8. Specialized equipment
9. Staging of material

Table 12 Operational Flying

a. Indicators Establishing Profiles

1. Aircraft density
2. Aircraft movement
3. Endurance capability
4. Flight history
5. Flight patterns
6. Force location
7. Force command control
8. Force composition
9. ICAO/FAA Flight plan information
    (a) Aircraft type
    (b) Airspeed
    (c) Altitude
    (d) Call sign
    (e) Course
    (f) Destination
    (g) Origin
    (h) Routing
    (i) Time of events
10. Low/high altitude operations
11. Mission characteristic features
12. Radar observation/detection
13. Refueling requirements/procedures
14. Sortie number
15. Sortie status
16. Tactical formation
17. Visual observation/detection

b. Indicators Showing Deviations

1. Camouflage
2. Search and rescue operations
3. Specialized aircraft
4. Weather limiting factors
5. Weather requests

(a) Addresses
(b) Frequency
(c) Location
(d) Priority

6. Weapons testing

Table 13 Personal Affairs

a. Indicators Establishing Profiles

1. Apparel
2. Child care services
3. Education program participation
4. Immunization records
5. Laundry services
6. Newspaper delivery
7. Passport
8. Personal equipment
9. Personal plans
10. Personal routine
11. Personal vehicle identification
12. Physical examination/tests
13. Purchase of personal effects
14. Security clearances
15. Spouse/dependent affairs and routine
16. Telephone services/directory listings

b. Indicators Showing Deviations

1. Advance payment
2. Billeting
3. Car rental
4. Change of address
5. Check-in/check-out of government quarters
6. Hotel/motel reservations
7. Mail forwarding
8. Permanent change of station
9. Personal arrangements for dependents
10. Personal arrangement for property care
11. Personal luggage
12. Power of attorney
13. Sale/purchase/rental of residence
14. Security investigation
15. Temporary assignment orders
16. Travel authorization/vouchers
17. Use of commercial transportation

18. Wills

Table 14 Personnel Activity

a. Indicators establishing Profiles

1. Specialist requirements
   (a) Assigned
   (b) By aircraft type
   (c) By equipment type
   (d) Shortages
2. Crew status
3. Apparel
4. Billeting arrangements
5. Crew proficiency
6. Manpower strength and projections
7. Medical/dental care routine
8. Name tags
9. Personnel activity
10. Personnel duty schedules
11. Personnel identities
12. Personnel location
13. Retention/reenlistment
14. Security investigation
15. Specialized personnel
16. Staff officer assignment
17. State of training
18. Unit patches
19. Unit strength

b. Indicators Showing Deviation

1. Casualty reports
2. Crew testing
3. Crew proficiency
4. Deployment orders
5. Education program modifications
6. Equipment/skill relationships
7. Immunization requirements/records
8. Manpower strength and projections
9. Medical/dental records
10. Mobility processing
11. Morale and discipline
12. Name tags
13. Off limits areas
14. Personal activity

15. Personal assembly
16. Duty schedules
17. Hiring/layoffs
18. Personal identities
19. Personal locations
20. Personal notifications
21. Personal recall
22. Physical examinations/tests
23. Retention reenlistment
24. Security investigations
25. Skill shortage
26. Small arms possession
27. Specialized personnel
28. Special manning
29. Special skill requirements
30. Special team deployment
31. Staff officer assignment
32. State of training
33. Survival training
34. Tailored training
35. Task qualification skills
36. Temporary duty funds
37. Termination of leave
38. Training
39. Travel reservations
40. Unfavorable personnel information
41. Unit activation
42. Unit patches
43. Unit strength

Table 15 Public Relations and Public Notices

a. Indicators Establishing Profiles

1. Background news articles and releases
2. Contractor advertisement
3. Legal/regulatory publication
4. Technical journal article
5. Security notices
6. Warning notices

b. Indicators Showing Deviations

1. Advertisement for bids
2. Advertisement for personnel hiring
3. Air space reservations

4. Environmental impact statements
5. Hazardous situation notices
6. Human situation notices
7. Human interest/hometown news release
8. ICAO/FAA flight plans information
9. News releases
10. Notice to airman-airspace restrictions
11. Personnel hiring/layoffs
12. Public appearances

Table 16 Schedules

Schedules serve to both establish profiles of normal activity and may identify deviations from normal profiles. Modifications to schedules are particularly Vulnerable to providing tip-offs.

1. Delivery/pickup schedules
2. Dining hall schedules
3. Distinguished visitors schedules an itineraries
4. Intelligence briefing schedules
5. Laundry service schedules
6. Leave schedules
7. Personnel duty schedules
8. Range schedules
9. Religious service schedules
10. Repair schedules
11. Senior officer schedules/itineraries
12. Test schedules
13. Training schedules
14. Transportation schedules
15. Vehicle schedules
16. Flying schedules
17. Maintenance schedules

Table 17 Services and Engineering Support

a. Indicators Establishing Profiles

1. Billeting capacity/use
2. Design factors
3. Dining hall operations
4. Electrical power requirements
5. Engineering studies
6. Environmental impact statements
7. Equipment availability/status
8. Firefighting capabilities

(a) Response time
(b) Operations

9. Laundry services /capabilities
10. Lighting
11. Provisioning
12. Road usage
13. Runway usage
14. Structural capabilities/design
15. Survival Equipment
16. Technical studies
17. Trash disposal
    (a) Disposal site
    (b) Schedule
    (c) Volume
    (d) Recyclable's

b. Indicators Showing Deviations

1. Billeting/service arrangements
2. Breakdowns
3. Camouflage
4. Damage assessments
5. Detectable pollutants
6. Environmental Profile
    (a) Heat
    (b) Lighting
    (c) Smoke/chemical aerosols/smells
    (d) Sound
7. Motel/hotel reservations/contracts
8. New construction
9. Runway/road closures degrades
10. Structure modifications

Table 18 System Capabilities

a. Indicators Establishing Profiles

1. Accuracy
2. Structural capabilities
3. Assessed threat to system
4. Design factor
5. Design features
6. Frequency range
7. Automated Information System(AIS)
    (a) Use
    (b) Dependency

(c) Alternatives
(d) Security
(e) Programming
(f) Types/models
(g) Capacities
(h) Product flow/volume
(i) Tempest status
(j) Emergency recovery procedures

8. Modes of operation
9. Name plate data
10. Operating instruction
11. Physical security system
12. Reliability
13. Security classification
14. Technical studies
15. Test equipment
16. Modems/internet/intranet

b. Indicators Showing Deviation

1. Communications system deployment
2. AIS system deployment
3. Modifications
4. Paint/preservative finishes
5. Performance degrades
6. System wide deficiencies/downgrades
7. Testing

EHXHBIT 14-2

COUNTERMEASURE TABLES

Table 1 Countermeasures to Cancel

a. Eliminate Indicators

1. Eliminate key events from tests, exercise and rehearsal to protect critical event sequences.
2. Simplify and thoroughly pre-plan procedures in detail to minimize the need for clarifying communications.
3. Modify functional responsibilities to decentralize control and information flow, allowing greater freedom of action without reports.
4. Eliminate routine reports: report by exception only.

5. Eliminate any operations/support related administrative calls on unsecured communications.
6. Use radio silence procedures in execution.

b. Conceal Indicators

1. Conceal unique features (physical and electromagnetic).
2. Conceal characteristic signature to conceal related activity.
3. Conceal tip-off indicators.
4. Time activities to occur during periods of minimum exposure to collection efforts.
5. Implement procedural changes.
6. Exercising under secrecy conditions even when not required both to train personnel and mask actual secret requirements.
7. Conduct all planning and coordination by secure communication.
8. Conceal agency or activity participation and operations support.
9. Conceal budgetary limitations.
10. Protect training status of forces.
11. Protect results of evaluations of tests, exercise and inspection.
12. Protect all systems modifications information.
13. Maintain strict need to know controls.
14. Don't process sensitive unclassified data on unprotected data processing systems.
15. Clearly identify classified and sensitive information so there is no doubt what requires protection.
16. Write complete, accurate detailed and realistic security classification guides supplements. Identify critical information in guides to assist guide interpretation and application. Ensure availability of the guide or portions to all participants.
17. Classify key tip-off indicator information.
18. Don't limit security classification because of current security clearances. Apply security classification criteria and definitions accurately, and upgrade security clearance as necessary.
19. Regularly review critical information and security classification guidance.
20. Protect key indicators in depth with security classification, concealment, masking operations, dissociation of key indicators and a cover story.

Table 2 Countermeasures to Confuse

a. Dissociation of Indicators

1. Avoid descriptive or easily associated projects/operation names, acronyms and nicknames.
2. Avoid standardized nicknames first words that identify the agency, department or major command.

3. Use generic terms rather than specific terms as titles and activity names, e.g., "Plans Office" rather than "Pacific Warplans Office".
4. Schedule operations/activity simultaneously so they mask each other; so associated activity relationships are confused to the observer.
5. Don't exercise critical events/activities in the true sequence.
6. Conceal the true relationship between tactics and procedures in exercises, training and actual planned tactics and procedures.
7. Periodically violate stereotyped procedures by unusual activities, exercise, and procedures(Do a boarding of a Navy Submarine that would get some peoples attention)
8. Create spurious indicators to degrade the value of true indicators as tip-offs.
9. Disrupt continuity of hostile communications intercept at key times in operations by simultaneous frequency/call sign/mode operations.
10. Disrupt associations between related activities and their support activities.
11. Script delay's hold times and time compressions into training plans to confuse timing/sequence analysis.
12. Use approved encoding procedures only. Discourage brevity codes, which might be perceived to provide security. (Prohibit brevity codes for sensitive information).
13. Have a credible cover story for sensitive operations so activities can be conducted normally without additional security measures.
14. Provide normal public release of cover story activities.

b. Reduce Contrasts

1. Create indicator stability whether there is or is not an operation.
2. Limit unique indicators and make unique activity appear to be conventional.
3. Add similar identifying features to other equipment to degrade uniqueness.
4. Use toned down identification markings on vehicles, aircraft and equipment.
5. Disrupt stability occasionally to mask real contrast or deviations in activity.
6. Maintain normal activity electronic and communication profiles during sensitive operations.
7. Maintain normal physical (including physical security) and personnel activity profiles during sensitive operations
8. Maintain normal activity symmetry during operations or disrupt normal symmetry occasionally to degrade predictability of profiles.
9. Group similar observable activities in timing, location, or sequence to alternative plans, operations, and normal activities to mask each other.
10. Maintain normal activity imagery profiles during sensitive operations.
11. Plan an operational mode of operations that has no significant contrast with normal activity but invalidates routine intelligence profile databases.
12. Dull activity level variations by gradual changes.
13. Modify patterns randomly over time.
14. Don't intensify or allow lulls in activity immediately prior to operations.
15. Periodically and overtly conceal non-sensitive material, equipment, aircraft and vehicle to dull perceptions that concealment is unusual.

16. Without disrupting normal profiles, time activity to occur during periods of least vulnerabilities.
17. Make checklists to make different activities look the same. Use common sequences and items whenever possible.
18. Initiate masking activities that are identical to operational activity.
19. Exercise at activities in a secure mode when secrecy is not required to train personnel and mask real activities.
20. When positive deviation or contrasts indicators must exist, create identical indicators at other times.
21. For each reiteration, of an operation modify events, countermeasures, and nicknames so they don't appear related.

c. Create Diversion

1. Create a high interest activity to draw attention away from sensitive operations.
2. Create observable tracks and trace indicators randomly to degrade interest in real operation track and trace indicators.
3. Mask activity at one location by increasing activity at another.
4. Launch operational missions at the same time and in the same manner as training.
5. Time all changes and security measures to cause maximum hostile confusion (if detection is not a factor) when confusion would be most costly to the adversary's operation or intelligence services.
6. Conduct exercises and training activity to mask sensitive operations.
7. Conduct inspections and training to mask sensitive operations.
8. Initiate exercise as diversions timed to mask actual operation preparations or deployment.

Table 3 Countermeasures to Deceive

1. Disguise indicators

a. Create indicators that foster ambiguous perceptions of purpose, objective, intentions and capabilities.
b. Project a message through open sources that is ambiguous, reinforcing both actual and deception plan objectives.
c. Intentionally leak, misleading information to neutralize the value of true information inadvertently revealed.

It is extremely important that the truthfulness and credibility of official public information sources remain beyond reproach. Public information agencies must never be asked to lie. In deception schemes, they should neither confirm nor deny, offering no comment.

d. Exploit the implicit purpose and the meaning of equipment, material and activities-use equipment for unsuspected or unusual purposes.

2. Create False Indicators

a. Conduct deception planning in conjunction with all training, even if plans are not used.
b. Establish the perception that deceptions are used, but without indicating how, when or where.
c. Infer confirmation **without actually lying** that capabilities or activities incorrectly conjectured by the media/press actually exist.
d. Create decoys to simulate key indicators of the operation when operations do not occur.
e. Prepare for operations along the lines of alternative operations that will not occur to create perceptions of alternative objective/intentions.
f. Conceal the extent of routine limitations in exercise of operational functions.
g. Cause perceptions faster than actual response by concealed pre-exercise activity.
h. Openly prepare responses the adversary expects, and then covertly do the unexpected.
i. Prepare deceptions that are compatible with operations, that are both logical and credible but not alluding to true intentions/objectives.
j. "Cry wolf" by conducting multiple deceptions that can be unmasked by the adversary to cause actual operation to appear as a deception.
k. Allow sufficient time for a deception to be interpreted, reported, and acted upon by the adversary.
l. Don't skimp on deception resources; the more resources devoted to a deception relative to an operation, the greater the credibility and effect.

CLASSIFIED INFORMATION MANAGEMENT PROGRAM EVALUATION CHECKLIST

A COMMENT IS REQUIRED IN THE COMMENTS SECTION FOR ALL ITEMS DEEMED "NOT APPLICABLE".

UNIT_____ DATE CONDUCTED:_____
COMMAND SECURITY OFFICER:_____
EVALUATOR:_____

PART 1 – Management

	PAGE REF	YES	NO
Does the unit hold the current Classified Information Management Program, COMDTINST M5510.23 and all effective changes?		____	____
Has a Command Security Officer (CSO) been designated in writing?	1-6, D.3	____	____
CMCO name_____			
Has a Classified Material Control Officer (CMCO) been designated in writing?	1-7, D.4	____	____
Has a Document Control Station Officer (DCSO) been designated in writing?	1-9, D.5	____	____
Does the unit have a promulgated information security plan?	1-6, D.3.c	____	____
Is the unit operating under a waiver or exception?	12-8, K	____	____
Is the waiver or exception valid and is a copy on file at the unit?	12-8, K	____	____
Is the unit reporting to the cognizant security manager the number of derivative classifications made each fiscal year?	2-4	____	____
Is a copy of the derivative classification report on file at the unit?	2-4	____	____
Does the unit maintain a copy of the "source list" with the file or record copy of derivative classification decisions involving multiple sources?	2-3, D.4.b	____	____

In a random sample of three unit personnel (excluding CSO, CMCO, DSCO, etc.) how many were aware of the requirement, and who to report to, for incidents involving sabotage, espionage, deliberate compromise or other subversive activities?	12.D.1	____	____
Are reports made and required action taken when individuals with access commit or attempt to commit suicide?	M5520.12A 3.A.3	____	____
Are required actions taken and reports made when an individual with access is absent without leave?	5520.12A 3.A.4	____	____
Are OPSEC countermeasures considered when planning operations?	14-3, B.1.e	____	____
Has an effective security education program been established?		____	____
Are all persons aware of the requirements to report compromise or subjection to compromise of classified information?	12-1, D.1	____	____
When a compromise, possible compromise or administrative discrepancy has occurred, is prompt investigative and other action taken to identify the source and reason and remedial action taken to ensure further compromise does not occur?	12-2, D.4.a	____	____
Do reports of incidents involving classified information contain all the required information?	12-3, D.4.b	____	____
Does the unit conduct an annual self evaluation and is that evaluation on file for two years?	1-6, D.3.d	____	____

COMMENTS:_____
_____
_____
_____
_____

EVALUATOR
COMMENTS:_____
_____
_____
_____
_____

PART II – Classification, Declassification and Downgrading

Number of derivative classifications made to date this fiscal year_____		
Review a recent derivative classification decision. Is the decision correct?	____	____

Do the CSO, CMCO, and DCSO understand the difference between Original classification and Derivative classification?	2-2, C-D	____	____
Do the CSO, CMCO, and DCSO know who the Coast Guard Original Classification authorities are and at what levels they are authorized to Classify?	2-2, C.3	____	____
Does the CSO, CMCO, and DCSO know how to tentatively classify material correctly?	2-6, J	____	____
Does the unit have an effective system to ensure prompt downgrading and declassification of material?	Chapter 10	____	____
Does the unit maintain a source list with the file copy of derivative classification decisions as required?	2-4, E	____	____
Does the unit review their classified holdings regularly and destroy unneeded material?	11-1, A.3	____	____

COMMENTS:_____
_____
_____
_____
_____

EVALUATOR
COMMENTS:_____
_____
_____
_____
_____

PART III – Marking

Is the “derived from” line properly completed?	3-2, C.2.c	____	____
Is the “declassify on” line properly completed?	3-2, C.2.d	____	____
Are documents properly marked with the overall classification, including page Markings?	3-2, C.2.b	____	____
Is portion marking used to show classifications of sections, parts, Paragraphs etc.?	3-2, C.2.a	____	____
Are subjects and titles of classified documents properly marked?	Chapter 3	____	____
Are transmittal documents marked to show the highest classification of any information being transmitted?	3-7, K.1	____	____
Are electronically transmitted messages marked properly?	3-4, E	____	____

Are documents containing foreign government information properly marked?	3-6, H	____	____

COMMENTS:_____
_____
_____
_____
_____

EVALUATOR COMMENTS:_____
_____
_____
_____
_____

PART IV – Access, Accountability and Control

Is access to classified material properly enforced by security clearance and Need-to-know?	6-1, A	____	____
Has the unit established the necessary control systems to account for Classified material?	6-2, B	____	____
Can classified material be retrieved in a timely manner?	6-1, B	____	____
Has a continuous chain of receipts been established for all Top Secret and Secret material?	6-1, B.1	____	____
Does the unit have a Security Control Point designated in writing?	6-2, C	____	____
Are Security Control Point and Document Control Station personnel cleared to the appropriate level?	1.5, D.1e	____	____
Are accountability records maintained for all Top Secret and Secret material?	6-3, E.2	____	____
Does the CMCO maintain a current roster of all persons who are authorized access to Top Secret information?	1-9, D.4.v	____	____
Does the Document Control Log contain all required information?	6-3, E.4	____	____
Are accountability records retained for the required period?	6-3, E.2	____	____
Are written procedures in place for the handling of incoming classified material?	6-5, G	____	____
Is incoming classified material inspected for evidence of tampering?	6-6, G.4	____	____
Is a record of destruction completed for Top Secret and Secret?	6-6, H.2	____	____

Are Top Secret disclosure records maintained?	6-7, J	____	____
Is the Top Secret disclosure record attached to each Top Secret Document or material?	6-7, J	____	____
Are correct inventory procedures followed?	6-7, K	____	____
Is the publication change check list utilized?	6-8, L & Ex. 6-1	____	____
Are page checks conducted at the appropriate times?	6-8, M.2	____	____
Are working papers marked, protected, and destroyed as required?	6-9, N.1	____	____
Is magnetic and optical media properly accounted for?	6-9, O	____	____
Are all disclosures of classified information outside the executive branch properly authorized?	7-2, B	____	____
Is proper authorization obtained prior to reproduction of classified material?	7-3, C.2	____	____
Are reproduced copies properly marked and accounted for?	7-3, C.3	____	____
Are copy machines authorized for reproduction of classified material located in a way so as to provide maximum security protection to the items being reproduced?	7-4, C.4.a	____	____
Are copy machines properly marked?	7-4, C.4.b	____	____
Have appropriate controls been instituted to preclude unauthorized Photography of classified information and equipment?	7-5, E.1	____	____
Is all classified material stored by approved methods?	Chapter 4	____	____
Are security containers inspected as required?	4-3, F	____	____
Are combinations changed when required?	4-4, G.3	____	____
Is an SF 700 maintained for each container or approved classified space used to store classified information?	4-5, G.5	____	____
Are combinations appropriately classified, stored and accounted for?	4-5, G.7	____	____
Are repairs to container conducted according to regulation?	4-5, H	____	____
Are containers kept locked when not actually in use or under direct observation by an authorized person?	4-6, I.2	____	____

Are Open/Closed signs being used on security containers?	4-6, I.3	____	____
Is the SF 702 being used on all security containers?	4-6, I.4	____	____
Are dust covers used on combination locks?	4-6, I.5	____	____
Is the shipping combination set on all retired security containers and locks?	4-4, G.4	____	____
Are classified cover sheets being used?	4-6, J.1	____	____
Does the unit have an EAP?	4-7, K	____	____
Are EAP drills conducted as required?	4-9, K.2.c	____	____
Are proper procedures followed when packing and addressing Classified material when sent?	8-6, H	____	____
Are suspense copies of document receipts kept as required?	8-8, I.4.b	____	____
Is tracer action taken when necessary for outstanding receipts?	8-8, I.4.b	____	____
Are individuals authorized to handcarry classified material designated in writing?	8-8, J.1.a	____	____
Are approved methods of destruction being used?	11-1, B	____	____
Are records of destruction signed by the destruction officials?	11-3, C.3.e	____	____
Is classified waste destroyed promptly?	11-3, D	____	____
Are proper visitor controls in place?	Chapter 5	____	____

COMMENTS:_____

EVALUATOR COMMENTS:_____

THIS EVALUATION CHECKLIST IS IN NO WAY INCLUSIVE OF ALL REQUIREMENT AND DOES NOT RELIEVE PERSONNEL FROM OTHER REQUIREMENTS NOT MENTIONED.