DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 5510.8F
N15
4 October 2001

COMSC INSTRUCTION 5510.8F

Subj: COMSC INFORMATION AND PERSONNEL SECURITY REGULATION

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) OPNAVINST 5239.1B

1. Purpose. To provide guidelines and procedures for implementing the personnel and information security program within Military Sealift Command (MSC) and its subordinate activities. This instruction outlines command responsibility for implementing the policy for the maintenance of the security of all classified information in the interests of national defense. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. COMSCINST 5510.8E.

3. Responsibilities. The Commander, Military Sealift Command (COMSC) is responsible for ensuring there is an effective Information and Personnel Security Program within MSC. In order to maintain an effective program, COMSC shall designate a Security Manager, Assistant Security Manager, Top Secret Control Officer (TSCO) and Information Systems Security Officer (ISSO) to manage the program.

4. Applicability. This instruction is applicable to all military and civilian personnel assigned to or employed at Headquarters, MSC and its field activities worldwide. Area Commanders must comply with this instruction, but may implement additional requirements as applicable.

//S//
JOHN B. STROTT
Chief of Staff

Distribution:
(See page 2)

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)
SNDL 41B (MSC Area Commanders)
41C (NFAF East/West)
41D (MSC Offices)
41E (APMC)
41K (COMAPSRON FOUR)
41L (COMPSRONs)
41M (MSC TAGOS Project Office & Detachment)

TABLE OF CONTENTS

TABLE OF CONTENTS *(Cont'd)*

TABLE OF CONTENTS *(Cont'd)*

CHAPTER 1

SECURITY OFFICE RESPONSIBILITIES

1-1 Introduction. The Commander, Military Sealift Command (COMSC) is directly responsible for ensuring that an effective Personnel and Information Security Program is established and maintained as directed by references (a) and (b).

1-2 Security Manager. The Military Sealift Command (MSC) Security Manager is responsible for the administration of the Personnel and Information Security Program either personally or through subordinates. He/she will:

a. Advise COMSC, whenever possible, regarding matters pertaining to the security of classified information and personnel security.

b. Ensure threats to security, compromises and other security violations are reported, recorded and when necessary, investigated. Report incidents involving security compromises to Naval Criminal Investigative Service Command (NCIS) and other incidents that come under the jurisdiction of NCIS. Report other incidents to the Naval District of Washington (NDW) Security Office and then to NCIS.

1-3 Assistant Security Manager. The Assistant Security Manager will report directly to the Security Manager, and in his/her absence, perform duties as Security Manager. He/she will:

a. Develop written Command Information and Personnel Security procedures.

b. Develop and coordinate the command's security education program.

c. Ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

d. Administer the command's program for classification, declassification and downgrading of classified information.

e. Control visits to MSCHQ and visits by MSC personnel to other commands.

f. Ensure that access to classified information is limited to those with a need to know.

g. Coordinate with the command Information Systems Security Officer (ISSO) on matters of common concern.

h. Maintain liaison with the Chief of Naval Operations (CNO) Special Security Officer concerning security investigations and eligibility for access to Sensitive Compartmented Information (SCI).

i. Ensure compliance with the Industrial Security Program for classified contracts with DoD contractors.

j. Ensure requirements of reference (b) are met when access to classified information is provided to contractors in connection with legitimate government business.

k. Ensure that personnel security investigations, clearances and access are recorded.

l. Establish a viable, ongoing security awareness program. This shall include training Program Manager/Functional Director Security Coordinators in their duties, as well as general awareness training to all hands. Training shall include the use of the POW, bulletin boards, HQ Online Editor and briefings to personnel.

1-4 Top Secret Control Officer. The Top Secret Control Officer (TSCO) is responsible to the Security Manager for receipt, custody, accounting for and disposition of Top Secret material at MSC Headquarters. The TSCO will:

a. Maintain a system of accountability of all Top Secret material located at MSC. The records will indicate source, downgrading, movement of Top Secret material from one office to another, current custodian and the destruction of the material or other disposition for which he/she is responsible.

b. Deliver material by direct contact to the person who will assume responsibility for it.

c. Maintain a continuous chain of signed receipts and disclosure records for all Top Secret material through person-to-person contact.

d. Ensure that all Top Secret material is accounted for and properly transferred when custodians and sub-custodians are relieved of their duties.

e. Ensure physical inventories of Top Secret material are conducted annually.

f. Maintain a roster of MSC personnel who are authorized access to Top Secret information.

1-5 Information Systems Security Officer. The ISSO is responsible for the protection of classified material processed on the automated systems/ computers.

1-6 NATO Control Officer. The NATO Control Officer maintains accountability of all NATO classified material within MSC. The NATO Control Officer will:

a. Maintain a roster of all MSC personnel who are read into the program.

b. Maintain the sub-registry for NATO material.

1-7 Security Assistant. The Security Assistant will provide assistance to the Assistant Security Manager in maintaining the Information and Personnel Security Program. He/she will:

a. Process security investigations for Confidential, Secret and Top Secret security clearances.

b. Provide guidance and assistance to the security guards in buildings 210 and 157.

c. Update the security guard orders as required.

d. Coordinate random security inspections for buildings 210 and 157.

e. Input and update data on the Access Control computer.

f. Test and replace batteries to fire alarms.

g. Provide security indoctrination for new employees.

h. Provide authorization letters for personnel requiring an MSC badge.

i. Maintain the Recall Roster of all MSC personnel.

j. Maintain a current MSC security clearance list and provide a copy to each Program Manager/Functional Director Security Coordinator.

k. Maintain the security combinations and/or date of change and custodians.

1-8 Program Manager/Functional Director Security Coordinator. Each Program Manager/Functional Director shall appoint a Security Coordinator, who will:

a. Provide security awareness training within the Program Manager/Functional Director staff.

b. Provide Recall Roster updates to MSC Security Assistant.

c. Prepare outgoing visit requests.

d. Review Program Manager/Functional Director security guidelines to ensure adherence to overall security program.

CHAPTER 2

PERSONNEL SECURITY

2-1 Access. Access is the ability and opportunity to obtain knowledge or possession of classified information. The dissemination of classified information orally, in writing or by other means shall be limited to those persons whose official duties require knowledge of that information. An individual will not have access to classified information simply because of the level of his or her security clearance. **No** individual shall be granted access to classified information solely by virtue of rank or position. Access is granted only on a need-to-know basis.

2-2 Personnel Security Clearances. Reference (a) outlines the requirements for granting a security clearance. Personnel security clearances shall be granted at MSC under the following conditions.

a. A memorandum must be sent to the MSC security office requesting a security clearance. All of information in Exhibit A **must** be provided.

b. There must be a valid investigation on file and applicable to the required clearance.

c. The individual must have had no more than a 24-month break in federal service.

d. There must be a favorable records check by the MSC security office before granting of a security clearance (Military Service record or civilian Official Personnel File).

e. Position Descriptions must be current and indicate sensitivity and requirement for level of clearance.

f. Interim clearances may be granted upon submission of required security investigation documents.

2-3 Access Control. MSC Headquarters and subordinate commands will establish a personnel security access listing which will be published at least monthly. This listing will include names of individuals, security clearance, type of investigation, date of investigation, date clearance was granted by MSC, and MSC code where assigned. A copy of this listing will be provided to each Program Manager/Functional Director/ Special Assistant who will make roster available to supervisors. This listing **will not** be incorporated into a notice but will be dated then provided to each Program Manager/ Functional Director/Special Assistant when changes occur.

2-4 Visit Control. COMSC is responsible for safeguarding classified information and for control of visitors within the command. Field activities may set up their own procedures in compliance with reference (a).

a. A visitor is:

(1) a person not a member of the MSC staff;

(2) a person not attached to or employed by the command or staff; or

(3) a person on temporary additional duty.

b. Classified/Unclassified Visits to other Commands/Agencies. When an MSC employee is to visit another Department of the Navy (DON) agency, government agency or contractor facility, the following procedures must be followed.

(1) The Program Manager/Functional Director Security Coordinator shall prepare a Visit Request (letter or message). The request must include the full mailing address, point of contact, telephone number and FAX number.

(2) A copy of the Visit Request shall be forwarded to the MSC Security Manager.

c. Incoming Classified/Unclassified Visits. Visitors to COMSC buildings 210 and 157 are granted access under the following conditions:

(1) U.S. citizenship is required for uncontrolled access to buildings 210 and 157.

(2) Visitors with security clearances are authorized access to classified information only when there is a valid contractual requirement.

(3) Citizenship of all visitors must be verified in writing by the COMSC Security Office. Non-U.S. citizens are not authorized unescorted access to buildings 210 and 157 and are not authorized access to sensitive or U.S. classified information unless approved by the U.S. Navy agency authorized to approve access.

(4) A visit request must be forwarded to MSC Security Office via fax or mail. Requests cannot be hand-carried by the visitor.

(5) Visit request must be on letterhead (company or activity) and signed by appropriate authority: i.e., Security Officer or Security Manager. Request must include the following personal data: name, rank social security number, date/place of birth, citizenship, purpose of visit, point of contact and security clearance.

2-5 Security Classification of Positions at MSC. Positions that are concerned with protection of the nation from foreign aggression or espionage are designated by position sensitivity. National security positions include those positions dealing with development of defense plans or policies, intelligence or counterintelligence activities and related activities concerned with the preservation of the military strength of the United States and positions that require regular access to classified information. There are three levels of position sensitivity and all positions at MSC are designated one of the following classifications:

a. Critical Sensitive. Requiring access to Top Secret information.

b. Non-Critical. Requiring access to Secret or Confidential information.

c. Non-Sensitive. Access to classified information is not required but employee suitability determination is required.

2-6 Security Investigation for Sensitive Positions. All investigative requirements must be met prior to employee or applicant being assigned to any sensitive duties. The results of the investigations must be received and reviewed by the Headquarters and/or field activity Security Manager prior to assignment of sensitive duties. Interim clearance may be granted initially for a 6-month period while waiting for final clearance determination.

2-7 New and Revised Security Classifications. Program Managers/Functional Directors/Special Assistants shall ensure the accuracy of security requirements of their subordinate positions. If a new position is established, or re-description of an existing position which involves a change in the incumbent's responsibilities, the following actions apply:

a. Item E of the Request for Personnel Action (SF 52) will be completed by the manager indicating the requirement for change in security classification.

b. If there is a requirement for security clearance in performance of the duties, the Position Description must be revised to reflect that requirement.

c. The Position Description will be reviewed by the Command Security Manager and classification specialist with recommendations made to the manager/supervisor/director as applicable to respective field activities. The Security Manger shall designate sensitivity level of positions in writing and in accordance with reference (a).

d. For all non-sensitive positions and re-description of existing positions not affecting a change in sensitivity of duties, the SF 52 will contain the statement **"There is no change in responsibilities."**

CHAPTER 3

CLASSIFICATION

3-1 Classification Designation. Information which requires protection against unauthorized disclosure in the interest of national security must be classified with one of the following designations per reference (b):

a. Top Secret. Information which could cause exceptionally grave damage to the national security if disclosed. Examples include:

(1) Armed hostilities against the U.S. or its allies;

(2) Disruption of foreign relations vitally affecting the national security;

(3) Compromise of national defense plans or complex cryptologic and communications intelligence systems;

(4) The revelation of sensitive intelligence operations; or

(5) Disclosure of scientific technological developments.

b. Secret. Information which could cause serious damage to the national security if disclosed. Examples include:

(1) Disruption of foreign relations;

(2) Impairment of a program or policy directly related to the national security;

(3) Revelation of significant military plans or intelligence operations; or

(4) Compromise of significant scientific or technological developments relating to national security.

c. Confidential**.** Information which could cause damage to national security if disclosed. Examples include:

(1) Compromise of information indicating strength of ground, air and naval forces;

(2) Compromise of performance characteristics;

(3) Compromise of test data;

(4) Compromise of production data on U.S. weapon of design; or

(5) Compromise of production data on U.S. weapon systems and munitions.

3-2 Authority to Classify, Downgrade and Declassify Material. Information classified by COMSC will be declassified as soon as it no longer requires protection in the interest of national security.

a. Original Classification Authority. The Secretary of the Navy (SECNAV) has designated COMSC as the only Original Classification Authority (OCA) for MSC. In COMSC 's absence, the person designated to act in his absence may exercise the classification authority. COMSC is designated as having OCA for:

(1) Top Secret Information. COMSC is designated OCA. Authority is limited to COMSC and can not be delegated.

(2) Secret Information. COMSC is **not required** to be designated but is authorized OCA because of Top Secret designation. Authority is limited to COMSC and can not be delegated.

(3) Confidential Information. COMSC is **not required** to be designated but is authorized OCA because of Top Secret designation. Authority is limited to COMSC and can not be delegated.

b. Derivative Classification. Derivative classifying is accomplished when information which is already classified is incorporated into a document, paraphrased, restated or generated in new form. If any of these actions have changed the level of or removed the basis for the classification, the originator will be asked to make a determination on the classification level of the document. The derivative classifier will also:

(1) Verify the current level of classification of information being used and will respect the classification decisions. Derivative classified documents should be marked at the level of the documents being used.

(2) On derivative documents, carry forward any previously assigned dates or events for declassification or note that information cannot be automatically declassified without approval from the originator.

CHAPTER 4

CLASSIFIED MATERIAL ACCOUNTING AND CONTROL

4-1 Basic Policy. COMSC and Area Commanders are responsible for establishing procedures for accountability of classified material received by their personnel and offices. Accounting limits the dissemination of and prevents unauthorized disclosure and reproduction of classified material.

4-2 Top Secret. Top Secret material shall be controlled by the Top Secret Control Officer (TSCO) in the following manner.

a. Incoming. Material will be:

(1) Page checked for completeness and accuracy when received;

(2) Entered into the command accountability register by the TSCO. The register will include changes, number of copies, serial number of document and will be marked to indicated copy number (i.e., copy 1 of 2); and

(3) Delivered internally hand to hand with signed receipts.

b. Filing. Retention of Top Secret material will be kept to a minimum and will be maintained until their purpose has been served. The TSCO will maintain a disclosure record (Exhibit B, OPNAV 5511/13) for each Top Secret document. The record will:

(1) Provide the title, name of individuals including stenographic and clerical personnel who have had access to/or have read the Top Secret material.

(2) Be signed by all who have had access to or have read the Top Secret material.

(3) Does not include those who have just had access to the container where the Top Secret material is stored or who administratively handle Top Secret material.

4-3 Secret. All Secret material will be accounted for by the mail room. Material received by individual or messengers should be referred to the contract operated mail room, delivered hand to hand and signed for in the mail room log system.

a. Incoming. Secret material will be controlled by the contract operated mail room. The following policies apply to all Secret material.

(1) When received by individual or messenger service, material will be hand delivered to the mail room and entered in the log system.

(2) When received by the mail room, material will be logged in the log system and signed for by an authorized employee.

(3) Under no circumstances will classified material be placed in an in/out box awaiting pick up.

(4) When routed through directorates, there is no requirement for signatures within the code, although the Director may establish a system of accountability as he/she believes necessary. When transferred to another directorate, there must be a transfer of custody through the mail room.

b. Filing. Retention of Secret material will be kept to a minimum and will be maintained until the purpose has been served.

4-4 Confidential. Custodians of Confidential material will provide safeguards to prevent unauthorized disclosure of the material.

a. Incoming. There is no requirement to maintain records of receipts, distribution or disposition of Confidential material.

b. Filing. Retention of Confidential material will be kept to a minimum and will be maintained until the purpose has been served.

4-5 Working Papers. Working papers are documents and material collected or created while preparing a finished document (i.e., rough drafts, classified notes, training course or conference notes).

a. When working papers contain classified information they will be:

(1) Dated when created.

(2) Conspicuously marked "**Working Paper**" on the first page in letters larger than the text:

(3) Marked centered top and bottom on each page with the highest classification of the information contained in the document.

(4) Protected in accordance with the classification assigned.

(5) When no longer needed, destroy in a manner approved by reference (b).

b. Accounting, controlling and marking requirements for a finished document will be followed when:

(1) Working papers contain Top Secret information;

(2) Are released by the originator outside the command, transmitted via email or fax or transmitted through message center channels within the command;

(3) Retained more than 180 days from the date of origin; or

(4) Filed permanently.

CHAPTER 5

REPRODUCTION OF CLASSIFIED MATERIAL

5-1 Basic Policy. Reproduction of classified material should only be conducted when there is an official requirement and not for convenience. Reference (b) requires that each command designate and mark copy machines for reproduction of classified material. COMSC has designated copy machines and there is no requirement for TEMPEST approved copy machines except where there is a Special Access Program (SAP). Where possible, two people will be involved in the reproduction process to ensure control and safeguarding of reproduced material.

5-2 Top Secret Material. Approval must be granted by the originating agency or higher authority before Top Secret material can be copied. Records will be maintained for a period of two years to show distribution of the material. The following procedures apply to MSC Headquarters:

a. When copies are made, each document will be annotated to show the copy number (i.e., copy 2 of 2).

b. The approval authority for reproducing Top Secret material at MSC is the Top Secret Control Officer (TSCO) or Alternate Top Secret Control Officer.

c. **No** copying of Top Secret material is authorized outside of the Communications Center.

5-3 Secret Material. Approval must be granted prior to copying Secret material. Classified material may be copied only on a copy machine designated for reproduction of classified material. A sign in the area of each copy machine will contain the level of classified material, if any, authorized for reproduction, and will identify those individuals who may authorize such reproduction.

5-4 Confidential Material. There is no requirement for approval of reproduction of Confidential material. Within MSC, Confidential material may only be reproduced on the copy machines designated for copying Secret material. When copying is complete, remove classified document and clear the machine by copying blank paper three or four times and then shred the paper.

CHAPTER 6

MARKING CLASSIFIED MATERIAL

6-1 Basic Marking Requirements. Classified material will be physically marked, annotated or identified by other means, as prescribed by the Department of the Navy (DON). The marking shall be in a manner that leaves no doubt about the level of classification assigned to the material. Anyone shall be able to determine which parts contain or reveal classified information, how long the material must remain classified and any additional measures necessary to protect the material. Marking requirements vary depending on the kind of material. Basic markings are required for all classified and are listed below.

a. Originally classified material must include:

(1) The original classification authority,

(2) The agency or office of origin,

(3) The overall classification of the document,

(4) The declassification date (OADR shall not be used in new documents) and

(5) Downgrading instructions.

b. Derivatively classified material will:

(1) Be marked or conspicuously stamped in capital letters (larger than those in the text) with the highest overall classification of any information contained in or revealed by the material.

(2) Include the agency and office of origin.

(3) Include the source of classification (original classification authorities, source document or classification guides or combinations) including the date for positive identification.

(4) If there were multiple sources indicate "Derived from multiple sources" and maintain a listing or documentation of the multiple sources.

(5) Include the declassification date or event (which must be no more than 10 years from the origination date of document) for declassification or state the 10-year automatic declassification exemption category(ies) listed in Exhibit B.

(6) Include downgrading action.

(7) Include warning notices or control markings from sources as applicable.

6-2 Page Markings on Correspondence. The basic markings will be placed on the first page of the correspondence. The overall markings will be typed at the upper left and stamped in the center at the top and bottom of the page. Classification authority, downgrading and declassification instructions will be placed at the lower left. Warning notices are spelled out after the typed classification at the upper left except for **RESTRICTED** or **FORMERLY RESTRICTED** Data. See Exhibit C for further instructions.

a. Portion Markings. If the classified document contains portions that are unclassified when standing alone, but classified when combined or associated with other portions, mark the page with the highest classification of any information revealed on the page. Mark the unclassified paragraphs as unclassified and the classified paragraphs at the level of information revealed.

b. Subjects and Titles. Whenever possible mark subjects and titles unclassified. When they are classified mark as following:

(1) Top Secret (TS)

(2) Secret (S)

(3) Confidential (C)

(4) For Official Use Only (FOUO)

(5) Unclassified (U)

c. Naval Messages. Classified messages are marked at the top and bottom with the overall classification and portion markings. The overall classification markings must be spelled out and, will be the first item of information in the text of a classified message. The last line of text must show the date or event for declassification.

CHAPTER 7

TRANSMISSION OF CLASSIFIED MATERIAL

7-1 Basic Policy. Transmission of classified material is the movement of classified information or material from one place to another. Transmission of classified material by commercial aircraft must be approved by the COMSC Security Manager. Area Commanders have the authority to approve escorting or hand-carrying of classified material on commercial passenger aircraft. The following policies apply to the movement of classified material:

a. Unless otherwise restricted, movement can either be by car, bus, train, ship or plane.

b. Movement of classified material across national borders is not permitted unless arrangements have been made to prevent inspections by customs and the postal service.

c. Foreign carriers may not be used to transport classified material unless the U.S. escort has physical control of the material.

7-2 Handcarrying Classified Material. The hand-carrying of classified material must occur when the material is urgently needed for a specific official purpose, there is a specific reason that the material cannot be transmitted by other approved means to the destination within sufficient time for the purpose and when it is mission essential. When classified material will be hand-carried, MSC employees must comply with the following procedures.

a. Employee must be designated, in writing, as a courier by the MSC Security Manager or Assistant Security Manager.

b. Employee must be courier briefed and a record maintained indicating a briefing was provided and subject understands the procedures.

c. Complete a DD 2501 (courier card) provided by the MSC Security Office for hand-carrying of classified material.

d. If hand-carrying classified material on commercial aircraft, a courier letter is required along with courier card. The letter must indicate full name of courier, agency, type of identification the individual will present, description of material being carried, (i.e., three sealed packages, 9” x 8” x 24”), addressee and sender; place of departure, destination (transfer points), date of issue and expiration date of letter (not to exceed 7 days from date of issue).

e. The courier letter must include the name, title and signature of the official issuing the letter.

7-3 Top Secret. Top Secret material will be transmitted by:

a. The Defense Courier Service.

b. The Department of State Courier System.

c. Cleared and designated MSC U.S. military personnel, government civilian employees or DoD contractors traveling on a conveyance owned, controlled or chartered by the government.

d. Cleared and designated U.S. military personnel or government civilian employees by surface transportation.

e. Cleared and designated MSC U.S. military personnel and government civilian employees on scheduled commercial passenger aircraft on flights outside the United States. For transmission of classified material, Area Commanders have the authority to approve the transmission of classified material.

7-4 Secret. Secret material will be transmitted by:

a. Defense Courier Service when U.S. control of the material cannot be maintained. (This does not apply to SCI and COMSEC material.)

b. The Department of State Courier System via registered mail to the State Department Pouch Room.

c. Appropriately cleared contractor employees within and between the United Sates and its territories when employees have the classified information under constant custody/protection at all times.

d. U.S. Postal Service registered mail within and between the United States and Territories.

e. U.S. Postal Service registered mail through Army, Navy or Air Force Postal Service facilities outside the area described in Chapter 9 (para.9-3) of reference (b).

f. Qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. Reference (b) outlines the restrictions.

g. Federal Express (FEDEX) or the current holder of the General Services Administration (GSA) contract for overnight delivery when approved by the official command mail control officer. The following restrictions apply to the transmission of classified material:

(1) Use of service is on an exception basis, when applicable postal regulations are met.

(2) An urgent requirement for overnight delivery for the executive branch to a DoD component or a cleared DoD contractor facility within the U.S. and its territories.

(3) The delivery service shall be U.S.–owned and U.S.-operated, provide automated in-transit tracking and ensure package integrity during transit.

(4) Sender shall ensure that an authorized person is available to receive the delivery and shall verify the correct address.

(5) Under **NO CIRCUMSTANCES** shall the release signature block on the receipt label be executed.

(6) The use of external (street-side) collection boxes is prohibited.

7-5 Confidential. Confidential material will be transmitted in one of the following manners.

a. U.S. Postal Service registered mail will be used:

(1) For NATO confidential.

(2) For mail to and from FPO and APO addressees located outside the United States and its territories.

(3) To other addressees when the originator is uncertain that their location is within the United States.

b. U.S. Postal Service First Class mail between DoD activities anywhere in the United States and its territories.

c. U.S. Postal Service certified mail or, if required by paragraph a above, registered mail to DoD contractors or non-DoD agencies of the Executive Branch.

d. Where available, U.S. Postal Service Express Mail Service between DoD activities and DoD contractors within the United States and territories.

e. Certified or registered must be used for mail to the State Department for forwarding by diplomatic pouch.

f. Commanders/Masters of ships of United States registry, who are U.S. citizens shipping classified material, must sign for the cargo and agree to:

(1) Deny access to the material by unauthorized persons including customs inspectors, with the understanding the cargo will not be unloaded.

(2) Maintain control of the cargo until a receipt is obtained from an authorized representative.

7-6 Telephone Transmission of Classified Material. Classified material will not be transmitted over the telephone except on approved secure communications circuits (STU III).

7-7 Preparation of Classified Material for Transmission. Classified material which is to be transmitted will be properly wrapped. Within MSC Headquarters, the mail room is responsible for ensuring material is prepared for transmission. Area Commanders must designate personnel to ensure compliance with reference (b). The following procedures apply.

a. Secret material will be prepared for transmission in a manner as to protect from unauthorized disclosure. When **mailing classified material**, it will:

(1) Be double wrapped and will be enclosed in two **opaque,** sealed envelopes or similar wrappings.

(2) Be addressed to an official government activity or DoD contractor. (Contractor facility clearance must be verified by the MSC Security Office prior to transmission.) Never address to an individual.

(3) Show the complete and correct address and MSC's address on the inner envelope or container. Consult the Standard Navy Distribution List (SNDL) to verify the mailing address.

(4) Be stamped, on the inner envelope, with the highest classification of the material enclosed.

b. If hand carried, a locked briefcase will serve as the outer wrapper or cover. During shipment of the classified material, under no circumstances will the material or package be left unattended in a closed and locked compartment of a vehicle or at a hotel overnight. Material must be delivered, without making any stops (i.e., at a hotel or home), to the nearest military installation for storage.

7-8 Transmission of Communications Security (COMSEC) Material. COMSEC material will be transmitted in accordance with reference (b). Material can only be transmitted through the Communications Security Material System (CMS). At MSC Headquarters the CMS Custodian and Alternate CMS Custodian are assigned to COMSC (N6). Area Commanders must comply with authorized security procedures in place.

a. Classified information will not be discussed or transmitted over the telephone except on approved secure communication circuits (STU III phones). Talking around a subject except on an approved secure line is prohibited.

b. Although MSC employees often use the phrase **"This is not a secure line",** the practice is not a Department of the Navy (DON) security requirement. The practice may be used at each office's discretion.

CHAPTER 8

SAFEGUARDING CLASSIFIED MATERIAL

8-1 Command Management. All MSC personnel are responsible for safeguarding classified material under their cognizance. The Security Manager is responsible for the administration of the Information Security Program. As required by reference (b), COMSC and each Area Commander shall designate a Security Manager who will implement the command's information security program.

8-2 Procedures. Anyone who has custody of classified material is responsible for safeguarding it at all times. The following safeguards must be followed to ensure compliance.

a. Secure classified material in Government Services Administration (GSA) approved security container when the material is not in use or under direct supervision by a employee who has the clearance and need-to-know.

b. Follow procedures to prevent unauthorized disclosure of the classified material by sight or sound.

c. Discuss the classified material only with a person who has a need-to-know or who has access to the classified material.

d. Classified material will not, under any circumstances, be removed from the office and taken home to work on.

e. A complete inventory log must be maintained for each security container. The following will be provided in the inventory:

(1) The document title

(2) Date originated or received by the command

(3) Date distributed or routed

(4) If routed, identify where and to whom

(5) Date of classification

(6) Control number if one was assigned

(7) Copy number if more than one copy

(8) If transferred identify where

(9) Date disposed of by the command and by whom

f. Do not remove classified material from directorates or working spaces except in performance of your official duties.

g. When hand-carrying classified material within the command office spaces, ensure that material is covered with one of the following classified material cover sheets:

(1) Standard Form 703 for Top Secret classified material

(2) Standard Form 704 for Secret classified material

(3) Standard Form 705 for Confidential classified material

h. After Hour Procedures

(1) Restricted Areas. Personnel working after hours on classified work must sign in and out on a log sheet.

(2) Clean Desk Policy. Each desk shall be double checked by the occupant and the last person to leave the office for the day. The purpose of which will be to ensure that all classified material has been properly secured.

(3) Store all classified material including classified waste, notes, plastic ribbons, rough drafts and electronically transmitted messages, regardless of the classification, in a GSA approved security container. Close the container and turn the dial at least four times to clear the combination. Try to open the container by turning the knob/handle and pulling the handle to open. If the container does not open then it is locked. Sign off on the Standard Form 702, Security Check Sheet, which should be attached to the container.

(4) In spaces where there is a security container, a Standard Form 701 must be posted and signed out by the last person to leave the office at the end of the day. It can be taped to the door or on the wall beside the door used as an exit. Each item on the list will be checked to ensure all classified material has been secured, as well as doors and windows. Although this is a standard form, additional requirements can be added at the discretion of responsible Commanders.

SAFEGUARDING CLASSIFIED MATERIAL IS AN ALL HANDS RESPONSIBILITY

CHAPTER 9

DESTRUCTION OF CLASSIFIED AND SENSITIVE MATERIAL

9-1 Basic Policy. Classified material shall be destroyed when there is no longer a requirement for maintaining the material. Each directorate will conduct an **annual clean out day** for the disposal of unnecessary classified material holdings. This does not apply to COMSEC material where there are additional security procedures. Area Commanders may set their own procedures as long as they are in compliance with reference (b). Headquarters will comply with the procedures outlined in this chapter.

9-2 Procedures for Destruction of Top Secret. All Top Secret material, rough drafts, memoranda, work sheets, masters, typewriter ribbons, computer disks and notes shall be turned over to the Top Secret Control Officer (TSCO) for destruction. Destruction will be by burn bag or approved cross cut shredder. The following procedures apply:

a. There shall be a record of destruction or an equivalent tracking report and a complete identification of the information being destroyed.

b. The destruction report will be dated and signed at the time of the destruction by two persons cleared for access at the Top Secret level. The record shall be maintained for 2 years.

c. Burn bags containing Top Secret material will be handled and accounted for at the Top Secret level until actually destroyed.

d. Burn bags for destruction at MSC Headquarters shall be hand delivered to COMSC (N6) for delivery to the incinerator for destruction of the material.

e. Material will never be left unattended but when required, store in an authorized security container or area until bag is taken to an incinerator for destruction.

9-3 Procedures for Destruction of Secret. Rough drafts of letters or documents, memoranda, masters, typewriter ribbons, notes and uncontrolled documents shall be disposed of in the following manner.

a. There shall be a record of destruction or an equivalent tracking report.

b. The destruction report will be dated and signed at the time of the destruction by two persons cleared for access at the Secret level. The record shall be maintained for 2 years.

c. Shred no greater than 3/64 inches wide by ½ inch long.

d. Pulverizers and disintegrators must have a 3/32-inch or smaller security screen.

e. Pulping devices with a ¼ inch or smaller security screen to destroy water-soluble material.

f. Burn bags containing Secret material will be handled and accounted for at the Secret level until actually destroyed. Persons accomplishing destruction are not required to sign the destruction report but must sign for number of bags destroyed.

g. Material will never be left unattended but when required, store in an authorized security container until destruction.

9-4 Procedures for Destruction of Confidential. COMSC and Area Commanders must comply with reference (b). The following policies apply to destruction of Confidential material and classified waste at MSC Headquarters.

a. Shredders located in buildings 210 and 157.

b. There is no requirement for a destruction report.

c. Burn bags containing Confidential material will be handled and accounted for at the Confidential level until actually destroyed. Material will never be left unattended but when required, stored in an authorized security container until the bag is taken to an incinerator for destruction.

9-5 Procedures for Destruction of Naval Messages. All Naval messages, regardless of the classification, shall either be shredded or burned in accordance with reference (b). Top Secret messages must be destroyed by the TSCO in a crosscut shredder or by burn bag, and a record of destruction completed.

9-6 Burn Bags. Burn bags containing classified material must be safeguarded in the same manner as the material itself. Burn bags shall be secured in an authorized security container until it is ready for destruction.

a. Each burn bag shall be labeled with name of individual responsible for the material, office code, phone number, building number and classification.

b. Burn bags shall only be filled halfway (not to exceed 10 pounds) and must be stapled closed.

c. N6 will conduct a burn run on the third Wednesday of each month. Material to be incinerated must be brought to the rear door (behind the guard desk) in the lobby of building 210 between 0800 and 0825 on the day of the run.

CHAPTER 10

SECURITY EDUCATION

10-1 Basic Policy. References (a) and (b) require MSC to establish and maintain an active security education program to instruct all personnel, regardless of position, rank or grade, in security policies and procedures. The Security Manager is responsible for providing training to all personnel. Area Commanders must comply with references (a) and (b).

10-2 Security Indoctrination. All personnel checking into MSC Headquarters must check in with the MSC Security Manager, where they will be provided a security indoctrination (MSC 5510/8 - Exhibit E). Supervisors and managers must ensure compliance. Without proper check-in, security clearances will not be granted. Area Commanders may set up their own procedures as long as it is in compliance with reference (a). Upon completion of the check-in process through COMSC (N11) or (N15) as applicable, all personnel (military and civilian) are provided training in the following areas of security:

a. Safeguarding classified information

b. Destruction of classified

c. Transmitting of classified

d. Security clearance and access procedures

e. Personnel in the information security program

f. Physical security procedures

g. Reporting of missing, lost or stolen government property

h. Courier procedures

i. Key and lock control

j. Marking of classified material

k. Transmission of classified material

l. Automated information security program

10-3 Refresher Briefing. All personnel at MSC Headquarters are provided an annual refresher briefing. The training will be designed for all that have access to classified material but shall be open to all that work at MSC. The training will advise employees of any changes in security programs as well as reemphasize current security requirements in personnel, information, industrial, automated information and physical security. Detailed requirements are provided in reference (a). Area Commanders may structure their training to meet the requirements of reference (a).

10-4 Counterespionage Briefings. As required by reference (a), once every 2 years all personnel who have access to Secret or above classified material must be provided a counterespionage briefing by an agent with the Naval Criminal Investigative Service Command (NCIS). The MSC Security Manager will arrange the training.

10-5 Special Briefings

a. Foreign Travel Briefings. Any MSC employee who has or has had access to classified information and is planning to travel outside the United States should contact the Security Office to schedule a briefing. The individual or the MSC Security Manager with NCIS can set up the briefings. Area Commanders should comply with this requirement but must set up procedures in compliance with reference (a).

b. NATO Briefings. All personnel at MSC who require access to NATO information must also be briefed by the NATO Control Officer.

c. Courier Briefings. Reference (b) outlines the procedures for hand-carrying classified material. Any MSC employee who transports classified material outside of the command must be briefed on the procedures to be followed while transporting classified material from one point to another. The courier will be provided a DD 2501 for local area and must be briefed on following procedures:

(1) **Do not** leave classified material unattended at any time or under any circumstances.

(2) Classified material must be in physical possession at all times unless properly stored at another United States government activity.

(3) If the trip involves an overnight stopover, advance arrangements must be made for storage at a government activity or cleared contractor facility.

(4) When material is surrendered, the courier must obtain a signed receipt from an authorized representative of the contractor facility or government installation.

(5) **Do not** read, study, display or use classified material in any manner on a public conveyance or in a public place.

(6) When carried in private, public or government conveyance, **do not** store in a detachable compartment such as automobile luggage rack, aircraft pod or drop tank.

(7) Provide your office, mail room or classified material control office with a list of all classified material carried or escorted by you. Upon your return, account for all classified material.

(8) Procedures for hand carrying classified on commercial aircraft.

10-6 Debriefings. All MSC employees who have had access to classified information will read excerpts from the Espionage Laws and Federal Statues and execute a Security Termination Statement (OPNAV 5511/14- Exhibit F) when there is no longer a requirement for access to classified information.

a. Debriefings will be conducted under the following conditions:

(1) Prior to termination from active military service or civilian employment or temporary separation for a period of 60 days or more.

(2) When a security clearance is revoked for cause.

(3) When a security clearance is administratively withdrawn.

(4) When an employee inadvertently received access to information for which he/she did not have the need-to-know and/or was not eligible to receive.

(5) When an employee is being transferred from one command to another.

b. During the debrief, the employee must be advised that:

(1) All classified material in their possession must be returned.

(2) He/she is no longer eligible for access to classified information.

(3) He/she may never divulge classified information, orally or in writing, or any unauthorized person without first receiving written permission from CNO (N09N).

(4) There are severe penalties for disclosure of classified to an unauthorized person.

(5) He/she must report to NCIS (or the FBI or nearest DoD component as applicable) any attempt by any unauthorized person to solicit classified information.

CHAPTER 11

INDUSTRIAL SECURITY

11-1 Basic Policy. Industrial security is that portion of information security, which is concerned, with the protection of classified information in the custody of U.S. industry. A classified contract is any contract, which requires or will require access to classified information by a contractor or his or her employees in the performance of the government contract. The contract may be classified even though the contract document is not classified.

11-2 Responsibilities of the Industrial Security Program at MSC Headquarters

a. The Security Manager has the responsibility for the Industrial Security program at MSC Headquarters.

b. The following procedures at MSC Headquarters are in place:

(1) Whenever there is a requirement for classified information to be released to contractors, the Security Manager shall verify whether the contractor has a facility clearance.

(2) The Security Manager makes verification of facility clearance through the Defense Investigative Service (DIS). If the contractor has a facility clearance, a request for documentation is requested at that time from DIS.

(3) If the contractor does not have a facility clearance, the Program Manager requesting the service, must initiate a DD 254 (Exhibit G) and submit via the MSC Security Manager to DIS.

CHAPTER 12

COMMAND SECURITY SELF-ASSESSMENT REVIEW

12-1 Basic Policy. MSC personnel conducting security self-assessment reviews must follow the guidelines included in the Command Security Self-Assessment Review Guide (Exhibit H). An expanded checklist is provided in reference (b). Area Commanders are urged to review and comply with the requirements outlined in reference (b) or, if requirements cannot be met, request a waiver.

12-2 Responsibilities for Management of Program. The Security Manager at each field activity must ensure that the security self-assessment reviews are conducted at least annually. Discrepancies shall be corrected to ensure compliance with reference (b). A copy of the review will be maintained for 3 years.

EXHIBIT A

SAMPLE OF REQUEST FOR SECURITY CLEARANCE

MEMORANDUM

From:
To: (Command Security Manager)
Via: (Appropriate Administrative Chain of Command)

Subj: REQUEST FOR SECURITY CLEARANCE

Ref: (a) COMSCINST 5510.8F

1. Per reference (a), the following information is provided for processing the below-designated individual's access to classified information up to and including (_____).

a. Name in full

b. Rank, rate or grade

c. Social Security Number

d. Date and place of birth

e. Position description number and title

f. Justification that the requested clearance is required for the proper performance of assigned duties

(Signature of Program Manager/Functional Director/Special Assistant)

(The information provided in this memo is to be safeguarded against unauthorized disclosure.)

EXHIBIT B

Duration of Classification

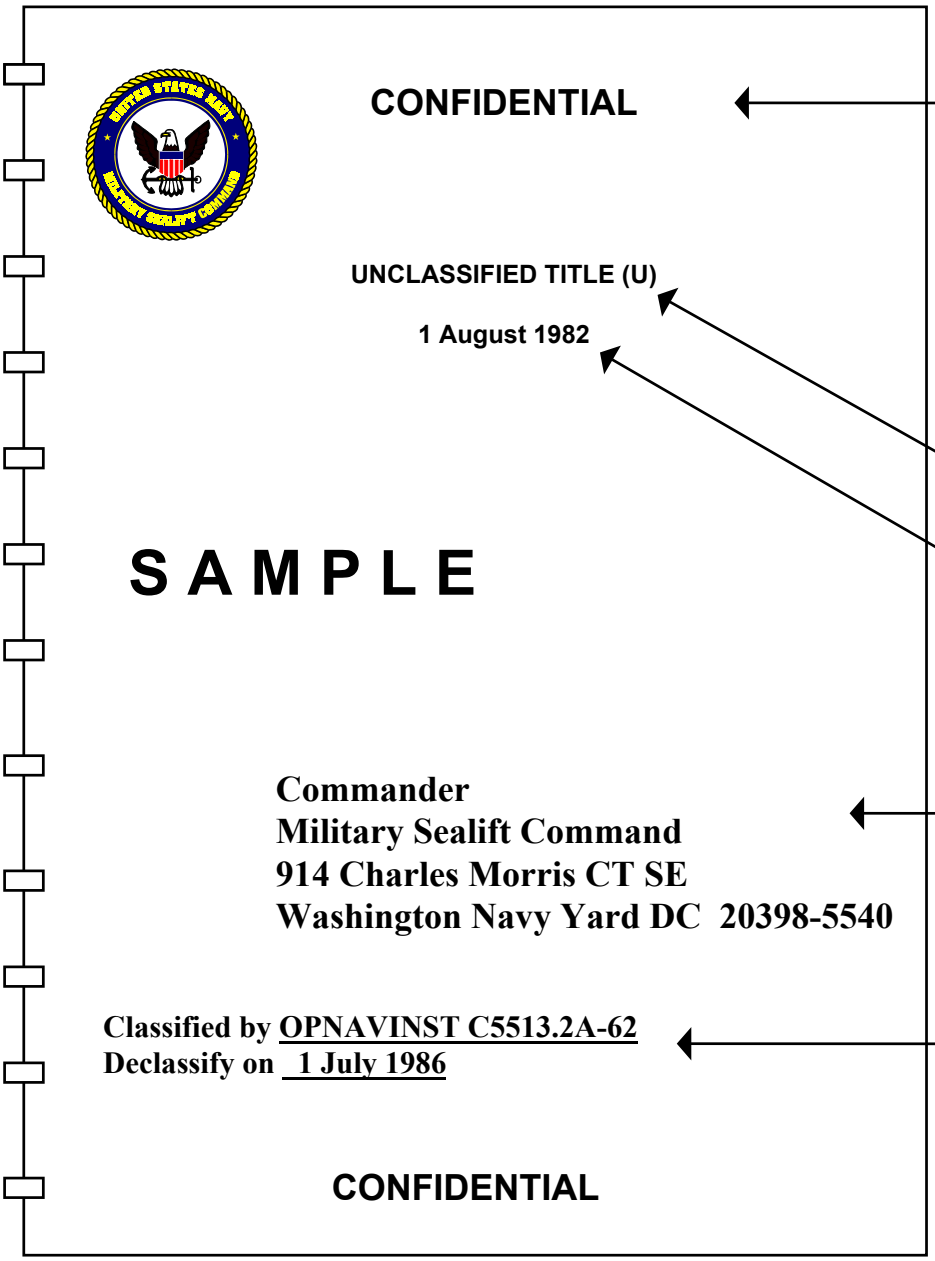
Declassification is the authorized changing of information from classified to unclassified. When information is originally classified, the classifier must identify a date or event upon which the information will be declassified. The standard in this Order is that information should normally remain classified for no longer than 10 years. But the Order also recognizes that there are some circumstances in which information must stay classified longer than 10 years because disclosure would cause damage to national security even after 10 years. The original classification authority may exempt information from the "10-year rule" if, even after 10 years, disclosure would be expected to:

- Reveal an intelligence source, method or activity, or a cryptologic system or activity *(X1)*
- Reveal information that would assist in the development or use of weapons of mass destruction *(X2)*
- Reveal information that would impair the development or use of technology within a United States weapons system *(X3)*
- Reveal United States military plans or national security emergency preparedness plans *(X4)*
- Reveal foreign government information *(X5)*
- Damage relations between the United States and a foreign government, reveal a confidential sources, or seriously undermine diplomatic activities that are reasonable expected to be ongoing for a period longer than 10 years *(X6)*
- Impair the ability of responsible United States Government officials to protect the President, the Vice-President, and other individuals for whom protection services, in the interest of national security, are authorized *(X7)*
- Violate a statute, treaty, or international agreement *(X8)*

The designators in parentheses following each item show the exemption categories specified in Section 1.6.d of the Executive Order. You'll need to know them when marking documents containing exempted information.

EXHIBIT C

COVER OF A PUBLICATION



A COMPLETE, PROPERLY MARKED FRONT COVER, TITLE PAGE OR FIRST PAGE

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

INTERIOR PAGES OF A DOCUMENT

SECRET

CHAPTER 5

FIRST ORDER HEADING (U)

Second Order Heading (U)

A. (U) Summary

1. (S) The classification marking of headings is illustrated above. Headings are marked according to their own classification and do not reflect the overall classification of the material which follows. Once a heading is identified by some means, it becomes a paragraph for marking purposes, e.g., "A. (U) Summary," as shown.

2. (U) The classification marking of paragraphs and subparagraphs is the same as for naval letter format. The classification of the lead-in portion of a paragraph is shown at the beginning of the paragraph even though a subparagraph may reveal a higher or lower level of classification.

a. (C) Subdivisions need not be marked if they do not express a complete thought. As an example, the following do not express complete thoughts:

(1) Systematized digital projection

(2) Compatible organizational flexibility

(3) Synchronized transitional contingency

b. (U) Individual paragraphs are classified according to the information they reveal.

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

SECRET

c. (S-NF) Intelligence control markings are shown on the front cover (if any), title page (or first page) and other applicable pages of a document. Interior pages will be marked with the short form of the control marking, that is NOFORN for Not Releasable to Foreign Nationals; WNINTEL for Warning Notice - Intelligence Sources or Methods Involved. Tables, figures and charts will be marked in a similar manner as illustrated in exhibit 9E. Paragraphs and subparagraphs will be marked with the abbreviated form such as NF for Not Releasable to Foreign Nationals; WN for Warning Notice - Intelligence Sources or Methods Involved, etc.

3. (U) The classification markings (top and bottom) should be bold and immediately distinguishable from the text and in red (in color) when practicable.

SAMPLE

2

SECRET/NOFORN

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

NAVAL LETTER

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON DC 20350

REFER TO:

5510
Ser 009p/S123456
1 August 1982

SECRET

From: Chief of Naval Operations
To: Recipients

Subj: PORTION MARKING (U)

1. (U) This is a sample of a fairly complex letter with multiple parts (paragraphs, subparagraphs and a chart). It has been created for the purpose of demonstrating the proper method of applying portion classification markings in accordance with the requirements of SECNAVINST 5510.30A. In this sample, paragraph 1 in its totality contains Secret information, but the lines of the opening paragraph do not, as indicated by "U" precursory marking.

a. (S) In continuing the graphic illustration of the proper techniques of applying portion classification markings, this subparagraph of the sample document contains information classified Secret as indicated by the "S" precursory marking.

(1) (S) Again, this subparagraph contains information classified Secret.

(a) (C) Every part of a classified document is to have portion classification markings applied. The text in this subparagraph contains information classified Confidential.

1. (S) The text in this subparagraph contains information that is Secret. Bear in mind that the objective of portion classification marking is to eliminate doubt as to which portions of a document contain or reveal classified information.

a. (U) This part of the sample document is unclassified as indicated by the "U" precursory marking.

b. (C) This part of the sample document is classified Confidential as indicated by the "C" precursory marking.

2. (U) This part contains no classified information.

Classified by OPNAVINST C5513.3A-17
Declassify on 4 Jan 1986

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

SECRET

Subj: PORTION MARKING (U)

(b) (C) The text in this subparagraph contains information that is classified Confidential.

(2) (U) The text in this subparagraph contains no classified information as shown by the "U" precursory marking. However, the information revealed by the chart that follows is classified Confidential.

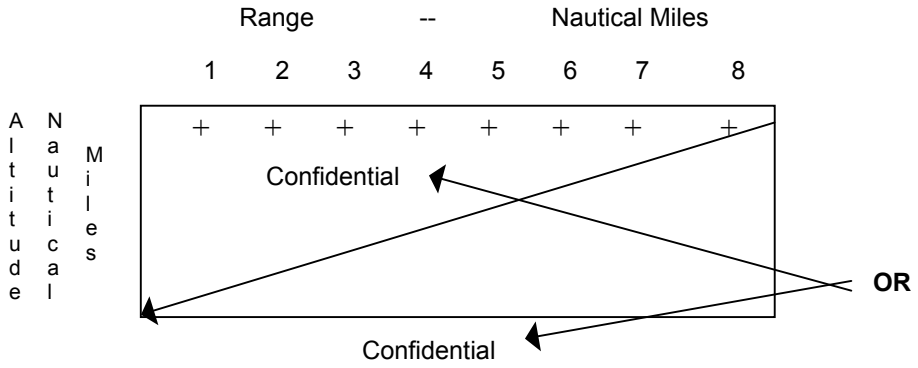


Chart No. 1 (U) Test Results

b. (U) If the above chart were to occupy an entire page, in a briefing book for example, it would still be necessary to mark separately the classification of the chart and its caption. The classification marking of the chart is so placed as not to be confused with the page markings. The text in this subparagraph is unclassified.

2. (U) It should be noted that this letter has been page marked according to its overall classification.

R. C. ALLEN
By direction

SAMPLE

2

SECRET

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

MEMORANDUM

CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON DC 20350

REFER TO:

5510
Ser 009p/C123456
1 August 1982

CONFIDENTIAL

MEMORANDUM FOR RECIPIENTS

Subj: PORTION MARKING SPECIAL FORMATS (U)

1. (U) Mark documents in a manner that eliminates doubt as to which of its portions contains or reveals classified information.

2. (U) There may be occasions when style or format considerations cause an arrangement of words that, standing alone, would not constitute a complete sentence. Normally, such word groups can be revised so as to make a single sentence or paragraph. The following two paragraphs are the same but are arranged differently to illustrate how to apply portion marking.

3. (C) Components of the F-99 aircraft system include:

   a. a signal processor;

   b. an emitter module;

   c. a high frequency receiver; and

   d. a cryptographic module.

4. (C) Components of the F-99 aircraft system include a signal processor, an emitter module, a high frequency receiver, and a cryptographic module.

5. (U) Subdivisions of the format in 3 above need not be marked if those subdivisions do not constitute a complete sentence. In the stylized format illustrated, there can be no misunderstanding or doubt that everything would be Confidential when taken together.

G. L. BERKIN
Head, Security Classification
Management Branch
Security Policy Division

Classified by OPNAVINST C5513.3A-16
Declassify on

CONFIDENTIAL

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

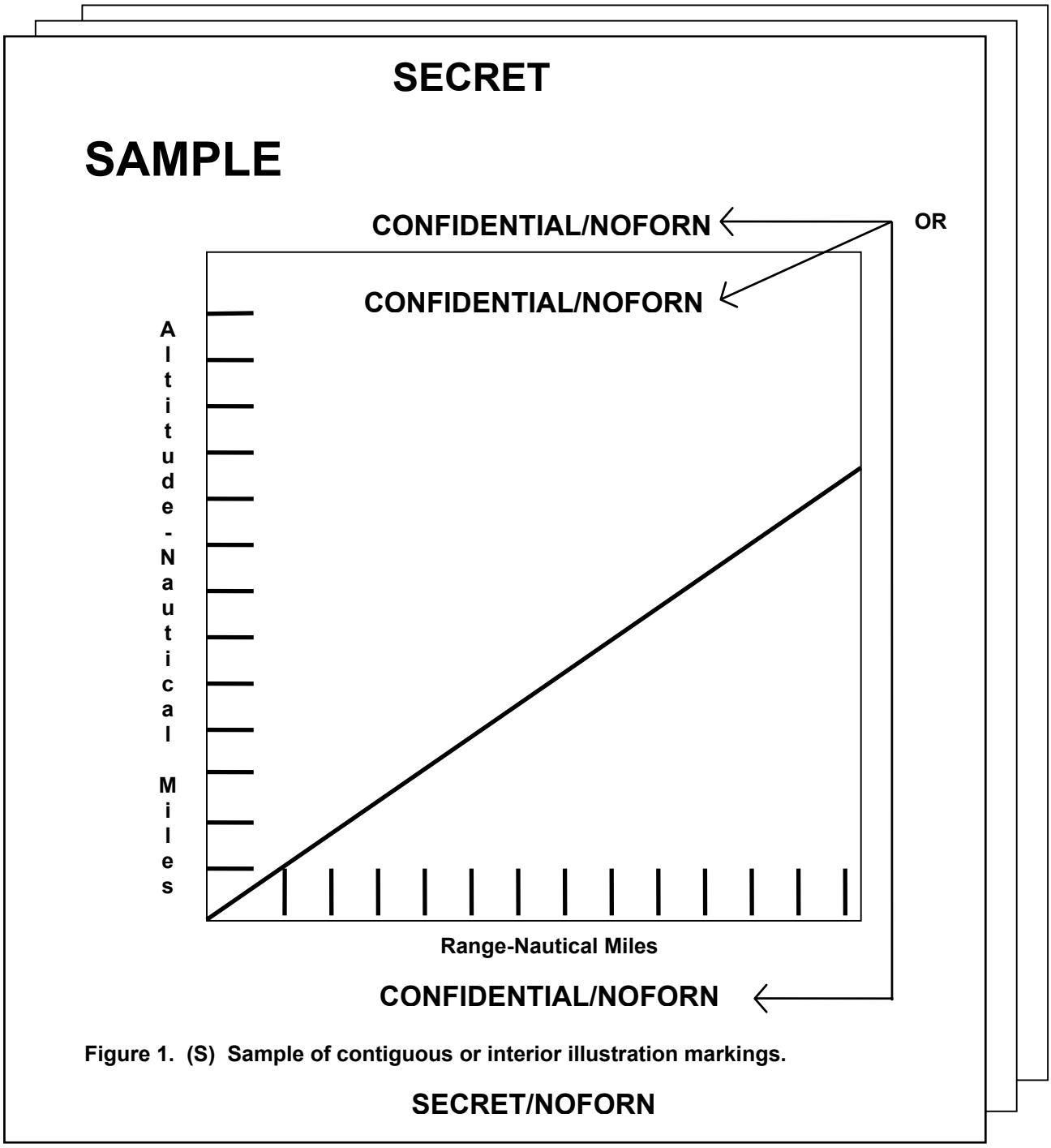


Figure 1. (S) Sample of contiguous or interior illustration markings.

Illustrations, figures, tables, graphs, drawings, charts and similar portions of classified documents must be clearly marked to show their classification. Place the marking close to, or within the illustration, etc., as shown above. Captions will be marked, on the basis of their own content, with the symbol (TS), (S), (C) and (U) immediately preceding the caption.

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

LETTER OF TRANSMITTAL

CONFIDENTIAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON DC 20350

REFER TO:

5510
Ser 009p/C123456
1 August 1982

CONFIDENTIAL -- Unclassified upon removal of enclosures (1) and (2)

From: Chief of Naval Operations
To: Commander, Naval Sea Systems Command

Subj: SECURITY CLASSIFICATION MARKINGS

Ref: (a) SECNAVINST 5510.30A
(b) CNO Washington DC 012345Z FEB 82

Encl: (1) NAVSEA Report 1410, The New Torpedo (U)
(2) List of Attendees
(3) NRL Report 1592, The Principles of Radar (U)

1. When titles or subjects of classified documents are included in the reference line, enclosure line or body of the letter, the classification of the title or subject follows, as shown on the enclosure line above. It is not necessary to show the classification of the reference or enclosure itself; however, each classified enclosure which must be removed before the letter of transmittal can be unclassified must be identified at the top, as shown.

2. Only the first page of an unclassified letter of transmittal carries classification markings. There would be no downgrading and declassification instructions on a letter of transmittal which is itself unclassified. If the letter of transmittal contains classified information, it will carry the appropriate downgrading and declassification instructions for the information it contains.

3. Intelligence control markings are typed out in full at the top, following the classification. If any enclosure contains Restricted Data, Formerly Restricted Data or Critical Nuclear Weapons Design Information, the words should be typed out after the classification at the top and the full warning notice placed at the bottom left. If the letter of transmittal contains information classified at the same level as the enclosure but does not, in itself, contain the information requiring the warning notice or intelligence control marking, words to the effect, "Warning notice (intelligence control marking) cancelled upon removal of enclosure (1)" should appear at the top.

ROBERT C. ALLEN
By direction

CONFIDENTIAL

NOTE: CONFIDENTIAL FOR TRAINING, OTHERWISE UNCLASSIFIED

MARKING OF CLASSIFIED U.S. MESSAGE TEXT FORMAT (USMTF) MESSAGES

1. E.O. 12958 has been interpreted to now require that messages be marked in a manner similar to documents. While the highly formatted and abbreviated nature of military messages introduces some eccentricities into the marking of messages, classified messages shall indicated (1) then nature of the classification (i.e., original or derivative), (2) the source of classification, (3) downgrading instructions (if applicable) and (4) declassification instructions (if applicable).

2. While messages continue to be marked with the highest overall classification level of the information contained in the message on the first line of text, as of 1 January 1999, the "DECL" set will be expanded to reflect the additional requirements of E.O. 12958. Prior to 1 January 1999, commands may implement this new "DECL" set in messages not automatically parsed by C4I systems. However, starting 1 January 1999, he updated 1999 USMTF User Formts Version 3.0 on CD-ROM will "drive" users to fill-in the appropriate fields. The "DECL" set will be formatted as follows:

"DECL/"

Field 1 (Derivative or Original Source (abbreviate as "**DERI:**" or "**ORIG:**" respectively) for Classification (this is a mandatory classification decisions are derivative))"/"

Field 2 (Reason for Original Classification (This field is mandatory if the previous field cites "ORIG" reflecting the rare occurrence of an original classification decision made by a DON OCA listed in **Exhibit 4A**. The allowable entries for this field are contained in Table 1))"/"

Field 3 (Downgrading and/or Declassification Instructions (to include declassification events) (abbreviate as "**INST:**") or Date (use "**DATE:**") (This field is "conditional," i.e., the "DECL" set will contain information in this field or field 4, but not both))"/" (with more data to follow) or "//" (to end the set).

Field 4 (Declassification Exemption Code ("X" Code) (This field is conditional, i.e., the "DECL" set must contain this field or field 3, but not both) (The allowable entries for this field or contained in Table 2))"/" (with more data to follow) or "//" (to end the set).

IMPORTANT NOTE: Fields 3 and 4 are *repeatable fields as a group* per USMTF rules (see examples 2, 4, 6 and 7).

(Field 2)

TABLE 1

(These "Reason Codes" parallel the seven E.O. 12958 classification categories, e.g., "15B" is equivalent to classification category "1.5(b)" of E.O. 12958)

REASON	
15A	Military plans, weapons systems, or operations
15B	Foreign government information
15C	Intelligence activities (included special activities), intelligence sources or methods or cryptology
15D	Foreign relations or foreign activities of the United States, including confidential sources
15E	Scientific, technological or economic matters relating to the national security
15F	United States Government programs for safeguarding nuclear materials or facilities
15G	Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security

(Field 4)

TABLE 2

(These are the 10-Year Automatic Declassification Exemption Codes from E.O. 12958)

"X" CODE	
X0	Classification was "OADR" prior to E.O. 12958 and classification guidance has yet to be revised to reflect appropriate "X" Code (Note: this code is rarely used)
X1	Intelligence source, method or activity, or a cryptologic system or activity
X2	Information that would assist in the development or use of weapons of mass destruction
X3	Information that would impair the development or use of technology within a United States weapons system
X4	United States military plans, or national security emergency preparedness plans
X5	Foreign government information
X6	Information that would damage relations between the United States and a foreign government, reveal a confidential source or seriously undermine diplomatic activities that are reasonably expected to be ongoing
X7	Information that would impair the ability of responsible United States Government officials to protect the President, the Vice President and other individuals for whom protection services, in the interest of national security, are authorized
X8	Information that would violate a statute, treaty or international agreement

3. The following are examples of completed "DECL" sets for classified USMTF messages:

EXAMPLE 1: SECL/DERI:MULTIPLE SOURCES/-/-X4//

NOTE: In this example, only the mandatory field (Field 1) and the conditional field (Field 4) have values to be reported. Hyphens are inserted to account for the other fields (Fields 2 and 3).

EXAMPLE 2: DECL/DERI:MULTIPLE SOURCES/-/-/X3/-/X4//

NOTE: In this example, because Fields 3 and 4 *are repeatable as a group*, a "no-value" hyphen must be inserted into the repeated Field 3 (this occurs after the "X3"). This must be done in order to insert the additional "X4" value into the repeated Field 4.

EXAMPLE 3: DECL/DERI:OPNAVINST S5513.5B-37/-/-/X3//

EXAMPLE 4: DECLL/DERI:USS BLYTHE 221023ZJUN1999/-/INST:DOWNGRADE TO (C) ON 26JUN1999/-/DATE:24DEC1999//

NOTE: Use a four-digit year as of March 1999. Also, see Note for Example 2.

EXAMPLE 5: DECL/DERI:CG-RN-1(REV 3)/-/INST:DO NOT DECLASSIFY//

NOTE: In this example, the information contained in the message is not only classified but is also RD. Since documents containing RD and FRD, do not bear declassification instructions, for messages containing RD or FRD, enter into Field 3 "INST:DO NOT DECLASSIFY//".

EXAMPLE 6: DECL/DERI:C7F OPORD JASWEX 2099/-/-/X3/-/X5//

EXAMPLE 7: DECL/ORIG:CINCPACFLT/15D/INST:DOWNGRADE TO (S) ON 24DEC1999/-/DATE:24DEC2007//

EXAMPLE 8: DECL/DERI:MULTIPLE SOURCES/-/-/X4//

EXAMPLE 9: DECL/DERI:CNO LTR N6 SER 9S263 OF 26MAY1999/-/-/X1//

EXAMPLE 10: DECL/ORIG:CNO(N87)/15A/-/X4//

EXAMPLE 11: DECL/DERI:USS KNOX LTR 5510 SER OC73243 OF 23MAY2000/-/-/X0//

EXAMPLE 12: DECL/ORIG:COMNAVSEASYSCOM/15A/-/X3//

EXAMPLE 13: DECL/DERI:USS EDGAR MARSHALL 240012ZDEC1997/-/ DATE:24DEC1998//

EXAMPLE 14: DECL/DERI:NORPAC FLEXOPS 99-3 LOI/-/INST:30 DAYS AFTER EXERCISE COMPLETION

NOTE: NAVADMIN 053/98 (NOTAL) included some inaccurate examples of original classification. This exhibit has been coordinated with CNO (N6).

JOINT MESSAGE FORM						SECURITY CLASSIFICATION SECRET SECRET				
PAGE	DTG/RELEASER TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG/MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
01 OF 01				RR	RR	SSSS				1231230
BOOK	MESSAGE HANDLING INSTRUCTIONS									

FROM: CNO WASHINGTON DC

TO: CINCPACFLT PEARL HARBOR HI

S E C R E T //N05510//

SAMPLE CLASSIFIED MESSAGE (U)

1. (S) CLASSIFIED MESSAGES WILL BE PARAGRAPH/SUBPARAGRAPH MARKED THE SAME AS NAVAL LETTERS.

2. (U) A "CLASSIFIED BY" LINE IS NOT REQUIRED. THE LAST LINE WILL SHOW, IN ORDER, DOWNGRADING DATA IF APPROPRIATE, THE ABBREVIATED DECLASSIFICATION DATE, OR THE NOTATION "OADR."

3. (U) THE ORIGINATOR'S RECORD COPY WILL INDICATE THE FULL DOWNGRADING/ DECLASSIFICATION MARKING AS FOR A DOCUMENT OR LETTER, INCLUDING SOURCES OF DERIVATIVE CLASSIFICATION. THE LAST LINE OF A MESSAGE, HOWEVER, NEED ONLY HAVE THE APPROPRIATE ELEMENTS IDENTIFIED IN PARAGRAPH 2 ABOVE, AS FOLLOWS:

DG/C/6JUN84 DECL: OADR

DISTR:

009P3

SC/009/NCC/IP

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE	SPECIAL INSTRUCTIONS	
MR. G. L. BERKIN, N009P3M 4-2230		
RELEASER: TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE		
RELEASER: SIGNATURE	SECURITY CLASSIFICATION SECRET	DATE TIME GROUP

NOTE: SECRET FOR TRAINING, OTHERWISE UNCLASSIFIED

MARKING GUIDE FOR PUBLICATIONS AND CORRESPONDENCE

(Refer to SECNAVINST 5510.30A for marking requirements for other types of material)

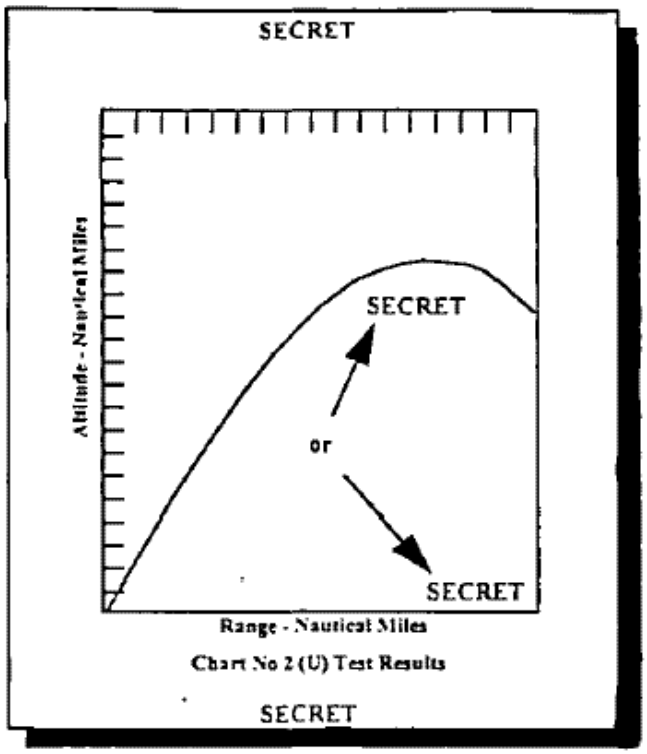
***Required Marking.**

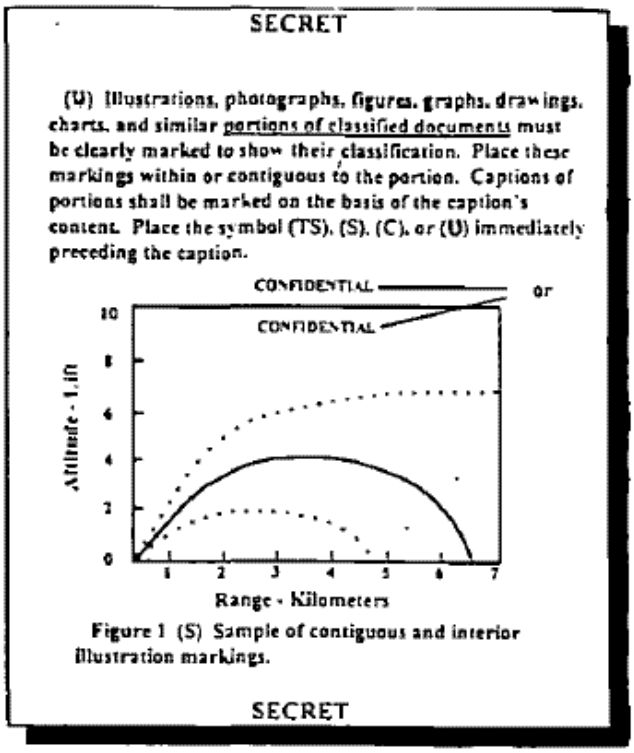
MARKING	PLACEMENT
*** Classification - TOP SECRET, SECRET OR CONFIDENTIAL**	**On publications, stamped or printed TOP and BOTTOM center in letters larger than other print, preferably in red, on the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). If the back cover is not used, classified text may not appear on the back of the last page. Mark interior pages of publications either with the overall classification or with the classification of the individual page. When exercising the individual page option in cases of front and back-printing, both sides of the page must be marked with the highest classification of either side. The side with the lower classification should be indicated at the bottom with the statement "This page is Unclassified" or other classification as appropriate.** **On the first page of correspondence, typed at the upper left in addition to the markings described above.**
*** CLASSIFIED BY (Insert)** **Insert the identity of the original classification authority or derivative classification source. (SECNAVINST 5510.30A lists original classification authorities; classification guides or other classified documents are derivative sources.) If more than one source is used, insert the phrase "Multiple Sources" and list all sources on the official record copy.**	**Once at lower left on the covering (first) page.**
*** DECLASSIFY ON (insert date or event or "OADR")** **Insert the declassification date or event. If neither of these can be predetermined, insert the notation "Originating Agency's Determination Required" or its abbreviation "OADR."**	**Once at lower left on the covering (first) page beneath the "CLASSIFIED BY" line.**
DOWNGRADE TO (Insert classification level) ON (Insert date or event)	**Once at lower left on the covering (first) page above the 'DECLASSIFY ON" line.**
(UNCLASSIFIED) (SECRET) or (CONFIDENTIAL) UPON REMOVAL OF ENCLOSURE (or specific enclosure, as applicable). This marking is required on letters or documents of transmittal which cover enclosures of a higher classification.	**Top left following classification marking (the classification marking must equal the highest classification of any enclosure being transmitted). Mark second and succeeding pages at TOP and BOTTOM center with the classification of the transmittal letter or document itself; if it is unclassified, no marking is required.**

MARKING	PLACEMENT
* AGENCY AND OFFICE OF ORIGIN (required if not otherwise evident).	Once on the covering (first) page.
DATE OF ORIGIN.	Once on the covering (first) page.
* (U), (C), (S), (TS) (required for all paragraphs, subparagraphs, titles, headings, captions, etc.). Naval nuclear propulsion information (NNPI) will not be portion marked.	Before each paragraph or portion (except NNPI), and before each caption. After headings and titles. (Use unclassified titles whenever possible to facilitate indexing.)
CLASSIFIED BY DOE-DoD classification guide CG-RN-1 dated January 1977. DECLASSIFY ON: Originating Agency's Determination Required. This document shall not be used as a derivative classification source (required marking for NNPI).	Once on covering (first) page.
WARNING NOTICES	
A RESTRICTED DATA This material contains Restricted Data as defined in the Atomic Energy Act 1954. Unauthorized disclosure subject to administrative and criminal sanctions (Full notice), RESTRICTED DATA (Short form), RD (Abbreviated form).	A Full notice at lower left on the covering (first) page beneath the "CLASSIFIED BY" line, in lieu of a "DECLASSIFY ON" line. Short form typed after classification at the top left on the first page of correspondence. Abbreviated form following portion marking classification symbol, e.g., (S-RD or S-FRD).
B Special Handling Required - Not Releasable to Foreign Nationals (Full notice) NOFORN (Short form) (May be applied to naval nuclear prolusion information (NNPI) only.) NOTE: An abbreviated form is not used because NNPI is not portion marked.	B On publications, full notice at lower left on the covering (first) page. On correspondence, full notice typed after the classification at upper left. Short form to identify tables, figures, charts, etc. Abbreviated form following the portion marking classification symbol, e.g., (S-RD) (N).
Critical Nuclear Weapons Design Information. DoD Directive 5210.2 applies (Full notice), CN WDI (Short form), (N) (Abbreviated form).	
C COMSEC Material - Access by contractor personnel restricted to U.S. citizens holding final Government clearance (Applied to COMSEC documents being released to contractors.)	C Once at bottom of covering (first) page.
Reproduction requires approval of originator or higher DoD authority.	

MARKING	PLACEMENT
Further dissemination only as directed by (insert name of activity) or higher DoD authority.	
This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be only with prior approval of the Naval Sea Systems Command. (May be applied only to classified or unclassified NNPI.)	
INTELLIGENCE CONTROL MARKINGS	
WARNING NOTICE - INTELLIGENCE SOURCES OF METHODS INVOLVED (Full marking), WNINTEL (Short form), WN (Abbreviated form).	**Full marking once at bottom center above classification marking on the front cover (if any), title page (if any) and first page of publication.**
NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR CONSULTANTS (Full marking), NO CONTRACT (Short form), NC (Abbreviated form).	**Full marking typed on the first page of correspondence following the classification at upper left.**
CAUTION - PROPRIETARY INFORMATION INVOLVED (Full marking), PROPIN (Short form), PR (Abbreviated form).	**Short form at top or bottom center of applicable pages, and for message classification lines, identification of tables, figures, charts, etc.**
NOT RELEASABLE TO FOREIGN NATIONALS (Full marking), NOFORN (Short form), NF (Abbreviated form).	**Abbreviated form following the classification designation in portion marking (e.g., (S-NC)).**
THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO (Insert specified country(ies)) (Full marking), REL TO ____ (Short form), REL (Abbreviated form).	
DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (Full marking), ORCON (Short form), OC (Abbreviated form).	

INTERIOR PAGES WITH A CHART





Charts, figures, tables, graphs and similar illustrations appearing within an interior page of a document shall be marked with their unabbreviated classification level and the short form(s) of applicable warning notice(s) and intelligence control marking(s), center top and bottom. Mark chart legends and titles with their abbreviated classification levels in parentheses immediately following them. Blueprints, engineering drawings, maps and similar items shall be marked in the same manner.

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
5510
Ser N09N2/9S123456
(Date)

SECRET

MEMORANDUM FOR THE DEPUTY UNDER SECRETARY OF DEFENSE (POLICY SUPPORT) (DUSD(PS))

Subj: FOREIGN GOVERNMENT INFORMATION (FGI) (U)

1. (FGI/C) Mark portions containing FGI to indicate the country of origin and the classification level. Substitute the words "FOREIGN GOVERNMENT INFORMATION" or "FGI" where the identity of the foreign government must be concealed. (While the identity of the foreign government source is concealed in the document, the identity is notated on the record copy and adequately protected. The "Derived from" line shall be marked "FGI source document dtd...").

2. (UK/S) This paragraph contains information considered "Secret" by the United Kingdom (UK). The "Derived from" line shall be marked "UK source document dtd..."

3. (U) FGI is exempt from the 10-year automatic declassification provision of E.O. 12958 under exemption "X5." Annotate the "Declassify on" line with "X5" and any other applicable exemption.

4. (U) The applicable warning notice shall be prominently placed at the bottom of the page.

B. S. GOLD
Special Assistant for
Security

Derived from: Multiple Sources
Declassify on: X5

"THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION" (for concealed foreign government sources); or

"THIS DOCUMENT CONTAINS (country) INFORMATION" (for foreign government sources identified)

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

SECRET

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
5510
Ser N09N2/9S123456
(Date)

SECRET

From: Chief of Naval Operations
To: Commander, Naval Air Systems Command

Subj: MARKING AN ORIGINALLY CLASSIFIED DOCUMENT (U)

Ref: (a) OPNAVINST 5513.1E of 16 Oct 1995

1. (S) Mark the face of an originally classified document with a "Classified by," "Reason," "Downgrade to" (if applicable), and "Declassify on" line. Include all applicable warning notices and intelligence control markings per paragraphs 6-11 and 6-12 of this regulation.

2. (U) A listing of "Reason" codes is found in reference (a).

DAVID L. BRANT
Special Assistant for
Naval Investigative Matters
and Security

Classified by: CNO (N09N)
Reason: 1.5a
Downgrade to: CONFIDENTIAL on 18 October 2000
Declassify on: 18 October 2001

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

SECRET

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER T

5510
Ser N09N2/9S123456
(Date)

SECRET

From: Chief of Naval Operations
To: Commanding General, Marine Corps Systems Command

Subj: MARKING A DERIVATIVELY CLASSIFIED DOCUMENT (U)

1. (S) Mark a document classified from a derivative source (e.g., a SCG, letter or report, etc.), with a "Derived from" lin instead of a "Classified by" line. Include a "Downgrade to" (if applicable), and "Declassify on" line with all applicable warnin notices and intelligence control markings per paragraphs 6-11 an 6-12 of this regulation.

2. (U) The majority of classified information is derivatively classified.

B. A. FITZ
Security Officer

Derived from: CNO ltr 5510
Ser 7U532200 of 20 Jan 97
Declassify on: 20 Jan 2006

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

SECRET

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
5510
Ser N09N2/9C123456
(Date)

SECRET--CONFIDENTIAL upon removal of enclosure (2)

From: Chief of Naval Operations
To: Director, Special Programs Office

Subj: CLASSIFIED LETTER OF TRANSMITTAL, TRANSMITTING A CLASSIFIED ENCLOSURE (U)

Encl: (1) CNO ltr 5510 Ser N09N2/7U12345 of 12 Oct 96
(2) CNO ltr 5510 Ser N09N2/7S12345 of 28 Sep 96

1. (U) A classified letter of transmittal shall be marked as any other classified document with all applicable associated markings.

2. (C) This classified letter of transmittal contains Confidential information and has a Secret enclosure, therefore, its highest overall classification level is Secret, but Confidential when the Secret enclosure is removed. Instructions to this effect are annotated on the face of the letter of transmittal, top left corner, as shown.

3. (U) The declassification instructions, bottom left, reflect the disposition of the Confidential information contained in the classified letter of transmittal after the classified enclosure is removed.

MARYANNE BATES
By direction

Derived from: OPNAVINST 5513.11B, enclosure (7)
Declassify on: Completion of test or 1 Jan 00

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

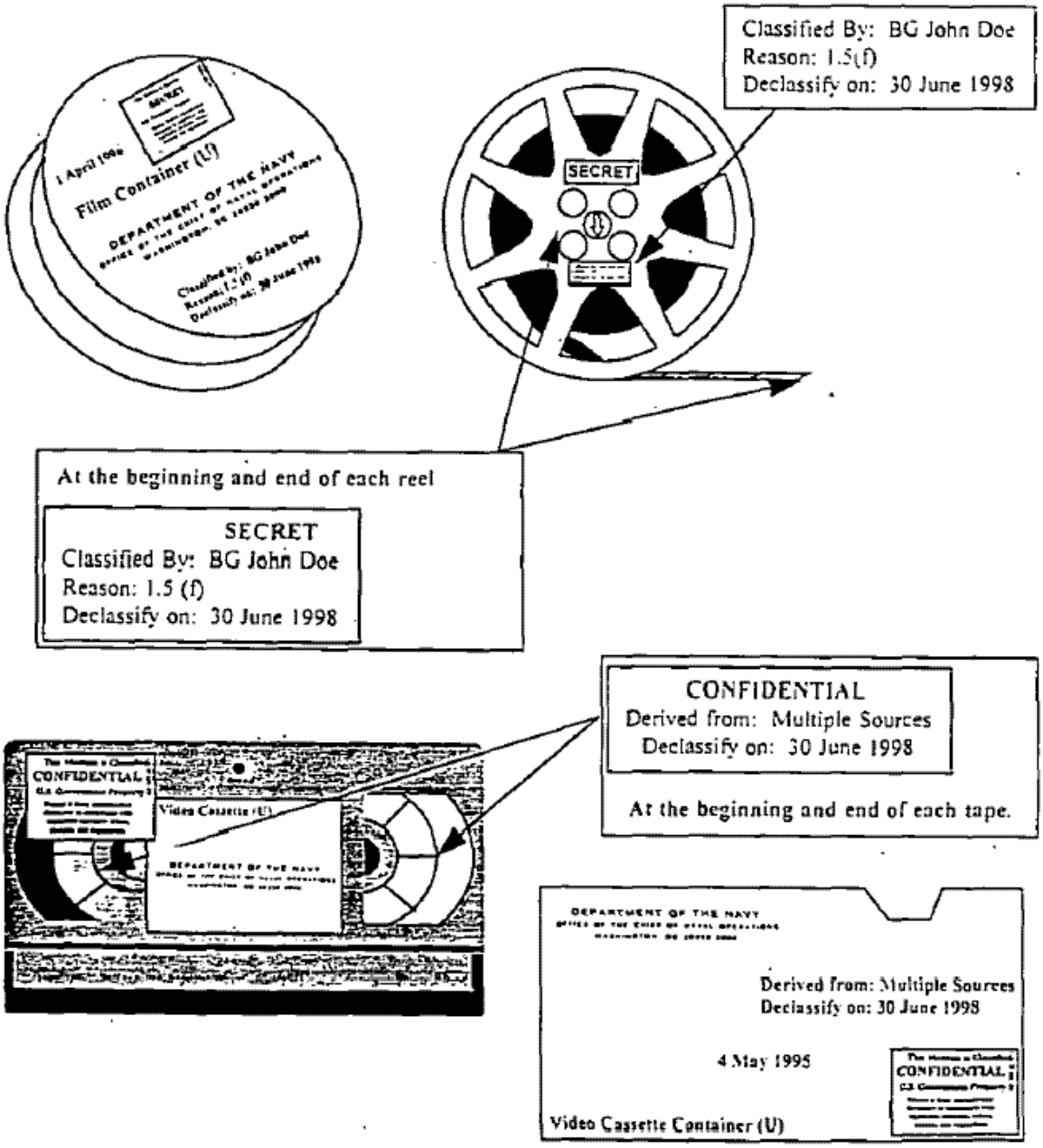
SECRET

ROLLED OR FOLDED DOCUMENTS

If rolled or folded, blueprints, maps, charts, or other large items shall be clearly marked to show their highest overall classification level.

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

MOTION PICTURE FILMS, VEDEOTAPES AND CONTAINERS



Classified motion picture films, videotapes and their titles shall be prominently marked, visible when projected, at the beginning and end of the production with the highest overall classification level and associated markings of the information they contain. Mark classified films, videotapes, and their containers in the same manner.

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" AND "CONFIDENTIAL" FOR TRAINING PURPOSES ONLY

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
5510
Ser N09N2/9U123456
(Date)

SECRET--CONFIDENTIAL Upon removal of enclosure (1)-Unclassified upon removal of enclosures (1) and (2)

From: Chief of Naval Operations
To: Commander, Naval Sea Systems Command

Subj: UNCLASSIFIED LETTER OF TRANSMITTAL WITH CLASSIFIED ENCLOSURES OR ATTACHMENTS

Ref: (a) Minutes of Naval Reactor Planning Group

Encl: (1) NAVSEA Report 1410, "The New Torpedo (U)"
(2) NRL Report 1592, "The Principles of Radar (U)"
(3) List of Attendees

1. Carry forward, to the face of an unclassified letter of transmittal, the highest overall classification level and the applicable warning notices and intelligence control markings per paragraphs 6-10 and 6-11, of its classified enclosures or attachments. It is not necessary to mark interior pages of unclassified letters of transmittal, however, they may be marked "Unclassified" for continuity.

2. Titles or subjects of classified documents included in the reference line, enclosure line, or body of a letter of transmittal shall be marked per paragraph 6-5. It is not necessary to indicate the classification level of the references or enclosures, however, each classified enclosure must be identified in the instructions at the top left corner of the transmittal as shown.

V. L. CICADA
By direction

THIS PAGE IS UNCLASSIFIED BUT MARKED "SECRET" FOR TRAINING PURPOSES ONLY

SECRET

EXHIBIT D

RECORD OF DISCLOSURE

OPNAV 5511/13 (REV. 1-76)
S/N 0107-LF-055-1165

TOP SECRET
(Unclassified when detached from document.)

ACTIVITY		**ACTIVITY CONTROL NO.**
ORIGINATOR	**COPY NO.**	**SERIAL NO.**

The attached material contains TOP SECRET information which bears directly upon the effectiveness of our national defense or the conduct of foreign relations. Because of its sensitivity, unauthorized disclosure can reasonably be expected to cause exceptionally grave damage to the national security. As such, the attached material deserves special care in its handling, custody, and storage, as required by the Department of the Navy Information Security Regulation, OPNAV Instruction 5510.1. This form is to be used as a record of persons who have read or had disclosed to them all or any part of the TOP SECRET information contained in the material identified above. This form is NOT A RECEIPT.

RECORD OF DISCLOSURE

Record below each person who sees, transmits, has custody of, or otherwise obtains knowledge of the TOP SECRET contents of the attached material.
DO NOT DETACH this Record of Disclosure unless the material is to be transmitted to another activity for retention.

ACTIVITY	FIRST AND LAST NAME	DATE	ACTIVITY	FIRST AND LAST NAME	DATE

TOP SECRET *(Unclassified when detached from document)*

CLASSIFIED MATERIAL DESTRUCTION REPORT
OPNAV 5511/12 (REV> 8-75) S/N 0107-LF-055-1160

CLASSIFICATION ***(Indicate when title or other identification is classified)***

TO:

FROM ***(Name and address of activity)***

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation, OPNAV INSTRUCTION 5510.1.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

SERIAL/DTG	ORIGINATOR	DATE	COPY NO.	LOG/ ROUTE SHEET NO.	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION ***(Signature, Rank/Rate/Grade)***

DATE OR DESTRUCTION

WITNESSING OFFICIAL ***(Signature, Rank/Rate/Grade)***

WITNESSING OFFICIAL ***(Signature, Rank/Rate/Grade)***

MSC CHECK-IN/CHECK-0UT SHEET

NAME:	GRADE/RANK/RATE:	SSN:	DATE:
COMPANY: *(For contractors only)*			

SEE INSTRUCTIONS ON THE REVERSE SIDE OF THIS FORM

OFFICE CODE	TITLE OF OFFICE	OFFICERS		ENLISTED		CIVILIAN		CONTRACTORS	
		IN	OUT	IN	OUT	IN	OUT	IN	OUT
N15	MILITARY PERSONNEL/SECURITY OFFICE *(Rm. 170 BLDG 210) MSC BADGE, RECALL BILL INFO								
	SECURITY BRIEFING *(Rm. 170 BLDG 210) SECURITY TERMINATION STATEMENT								
N002	FLAG SECRETARY (Rm. 404, BLDG 210)								
N14	COMMAND SENIOR ENLISTED ADVISOR (Rm. 170, BLDG 210)								
N11C	COMMAND CAREER COUNSELOR (RM. 170i, BLDG 210)								
N12d	PERSONNEL (Rm. 170R, BLDG 210)								
N13	TRAINING ADMINISTRATOR *(Rm. 185F, BLDG 210)								
N00R	RESERVE PROGRAMS (Rm. 170, BLDG 210)								
N0021A	MAIL ROOM (Rm. 105, BLDG 210)								
N0021	CLASSIFIED DIRECTIVES (Rm. 110, BLDG 210)								
N431B	PROPERTY MANAGER (Rm. 125, BLDG 210)								
N65	PHYSICAL FITNESS COORD (Rm. 225-4, BLDG 210)								
N65	CLASSIFIED LAN (Rm 200, BLDG 210)								
N6221	TOP SECRET/CMS CUSTODIAN (Rm. 300, BLDG 210)								
N65H3	TELECOMM SPECIALIST (Rm 335-2, BLDG 210)								
N311B	SENIOR WATCH OFFICER (Rm. 375, BLDG 210)								
N3/5FP	COMMAND FORCE PROTECTION OFFICER (Rm. 365, BLDG 210)								
N2	OFFICE OF GENERAL COUNSEL (Rm. 425, BLDG 210)								
N00P	PUBLIC AFFAIRS (RM. 465, BLDG 210)								
N9	FOIA/PRIVACY ACT (Rm. 470, BLDG 210)								
N00A	FORCE MASTER CHIEF (Rm. 485, BLDG 210)								
N82	ACCOUNTING OFFICER (Rm. 435, BLDG 157)								
N852	BANK OF AMERICA CREDIT CARD COORDINATOR (Rm. 475, BLDG 157)								
N732	SAFETY (Rm. 375A, BLDG 157)								
N10	GOVERNMENT PURCHASE CARD (Rm. 235, BLDG 157)								
N101	SPS SYSTEMS ADMINISTRATOR (Rm. 245, BLDG 157)								
N _____	OFFICE HEAD (Rm. _____ BLDG _____)								
N65	CSC HELP DESK (Rm. 360, BLDG 210)								

N15	**FOR ALL MILITARY, CIVILIANS AND CONTRACTORS** LAST STOP BEFORE DETACHMENT - MSC SECURITY OFFICE (Rm. 170, BLDG 210). RETURN DoD/MSC BADGE AND COURIER PASS. SIGN SECURITY TERMINATION STATEMENT, AND REMOVE FROM SAFE CUSTODIAN LISTING. UPON COMPLETION OF CHECK-IN/CHECK-OUT RETURN THIS FORM TO THE SECURITY OFFICE (N15), ROOM 170 BLDG 210.

PRIVACY ACT STATEMENT

AUTHORITY FOR COLLECTING ANY INFORMATION IS 10 USC 5031, PROVIDING THE REQUESTED INFORMATION IS VOLUNTARY. THE INTENDED USE IS FOR THE ADMINISTRATIVE PERSONNEL OFFICE AND WILL BE KEPT ON FILE FOR OFFICIAL USE ONLY.

All personnel will complete the appropriate sections of this form no later than five (5) working days after reporting on board COMSC and prior to detachment from COMSC.

Upon completion of Check-in/Check-out return this form to the Security Office (N15), Room 170 BLDG 210.

When Checking in N15 is first stop.

When Check out N15 is last stop.

With the exceptions listed below, Check-in/Check-out will be done in person. Since the Command is located in more than one building, ample time should be set aside to complete Check-in/Check-out procedures.

When checking in/out Military Personnel:

- Check-in/out with Naval Medical Clinic, WNY, BLDG 183 (Report in with Medical Record) Dental Clinic, WNY, BLDG 166 (Report in with Dental Record)
- Check-in/out with PSD, Anacostia, BLDG 92, Anacostia (Report in with Service Record)

Unless otherwise directed at the time of Check-in/out the following offices may be contacted by phone.

Classified Directives Control (N0021)	685-5092
Deputy EEO Officer (N00IE)	685-5987

SECURITY TERMINATION STATEMENT

Commander
Military Sealift Command
914 Charles Morris CT SE
Washington Navy Yard DC 20398-5540

1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (SECNAVINST 5510.30A) and the Communications Security Material System Manual (SMSM) in that I have returned to the Department of the Navy all classified material which I have in my possession.

2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.

4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I _____ have been informed and am aware that Title 18 U.S.C., Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understood appendix F of the Information Security Program Regulation SECNAV Instruction 5510.30A. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.

6. I have/have not received an oral debriefing.

SIGNATURE OF WITNESS	**SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE (Fill in first, middle, and last name. If military, indicate rank or rate. If civilian, indicate grade.)**
TYPE OR PRINT NAME OF WITNESS	**DATE**

EXHIBIT H

DEPARTMENT OF DEFENSE **CONTRACT SECURITY CLASSIFICATION SPECIFICATION** **(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)**	**1. CLEARANCE AND SAFEGUARDING** a. FACILITY CLEARANCE REQUIRED b. LEVEL OF SAFEGUARDING REQUIRED

2. THIS SPECIFICATION IS FOR: *(x and complete as applicable)*		**3. THIS SPECIFICATION IS**: *(x and complete as applicable)*		
☐ a. PRIME CONTRACT NUMBER		☐ a. ORIGINAL (Complete date in all cases)		Date (YYMMDD)
☐ b. SUBCONTRACT NUMBER		☐ b. REVISED (Supersedes all previous specs)	Revision No.	Date (YYMMDD)
☐ c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYMMDD)	☐ c. FINAL (Complete Item 5 in all cases)		Date (YYMMDD)

4. **IS THIS A FOLLOW-ON CONTRACT?** ☐ YES ☐ NO. If Yes, complete the following:

Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.

5. **IS THIS A FINAL DD FORM 254?** ☐ YES ☐ NO. If Yes, complete the following:

In response to the contractor's request dated _____ retention of the identified classified material is authorized for the period of _____

6. **CONTRACTOR** (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

8. ACTUAL PERFORMANCE

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	**YES**	**NO**	**11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:**	**YES**	**NO**
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			**a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY**		
b. RESTRICTED DATA			**b. RECEIVE CLASSIFIED DOCUMENTS ONLY**		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			**c. RECEIVE AND GENERATE CLASSIFIED MATERIAL**		
d. FORMERLY RESTRICTED DATA			**d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE**		
e. INTELLIGENCE INFORMATION:			**e. PERFORM SERVICES ONLY**		
(1) Sensitive Compartmented Information (SC)			**f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES**		
(2) Non-SC			**g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER**		
f. SPECIAL ACCESS INFORMATION			**h. REQUIRE A COMSEC ACCOUNT**		
g. NATO INFORMATION			**i. HAVE TEMPEST REQUIREMENTS**		
h. FOREIGN GOVERNMENT INFORMATION			**j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS**		
i. LIMITED DISSEMINATION INFORMATION			**k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE**		
j. FOR OFFICIAL USE ONLY INFORMATION			**l. OTHER (Specify)**		
k. OTHER (Specify)					

DD Form 254, DEC 90 **Previous editions are obsolete.** **S/N 0102-LF-011-5800**

12. **PUBLIC RELEASE**. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

☐ Direct ☐ Through (Specify):

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE**. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fi8ll in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) ☐ YES ☐ NO

15. **INSPECTIONS**. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) ☐ YES ☐ NO

16. **CERTIFICATION AND SIGNATURE**. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (include Area Code)

d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION
	☐ a. CONTRACTOR
	☐ b. SUBCONTRACTOR
	☐ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINSTRATION
	☐ e. ADMINISTRATIVE CONTRACTING OFFICER
	☐ f. OTHERS AS NECESSARY

DD Form 254 Reverse, DEC 90

EXHIBIT I

MILITARY SEALIFT COMMAND
COMMAND SELF-ASSESSMENT REVIEW GUIDE

Functional Area: Security

Activity: _____

Inspection Date: _____

Inspector: _____

Functional Area Evaluation: SAT: _____ UNSAT: _____

References: (a) SECNAVINST 5510.30A
(b) OPNAVINST 3120.32B
(c) SECNAVINST5510.36

A. General Administration:	**YES**	**NO**
1. Review of Tabs from the last inspection:		
a. Was action completed on all Tabs and the record closed?	_____	_____
b. Has the action taken solved the problem?	_____	_____
c. Is further action required?	_____	_____
2. Personnel issues:		
a. Is the number and composition of the staff adequate to handle the workload?	_____	_____
b. Are position descriptions accurate/current and do employees have copies?	_____	_____
c. Are all employees covered under an approved performance plan?	_____	_____
Do employees have copies?	_____	_____
d. Is outstanding performance recognized and are remedial steps taken to improve poor performance?	_____	_____
e. Has required training been received?	_____	_____
3. Is the work environment satisfactory?	_____	_____
a. Office space, furniture, equipment?	_____	_____
b. Heat, air conditions, ventilation?	_____	_____
c. Storage?	_____	_____

Comment:

_____

_____

_____

B. Program Management	YES	NO
1. Does the command hold the current edition of reference (a)?	_____	_____
2. Is the security manager designated in writing and identified by name to all of the command personnel?	_____	_____
3. Is the Top Secret Control Officer designated in writing?	_____	_____
4. Is the Top Secret Security Manager designated?	_____	_____
5. Is an Information Systems Security Officer (ISSO) designated?	_____	_____
6. Do the ISSO and the Security Manager coordinate and cooperate in the command program?	_____	_____
7. Are command security procedures in writing and current?	_____	_____
8. Does the command have a current written emergency plan and is an emergency destruction plan included where required?	_____	_____
9. Are security functions performed by another activity covered by a written security servicing agreement?	_____	_____
10. Does the command have an effective security education program?	_____	_____
11. Are indoctrination briefings given?	_____	_____
12. Are orientation briefings given?	_____	_____
13. Is on-the-job training given?	_____	_____
14. Are annual refresher briefings given? Date of last briefing _____.	_____	_____
15. Are counterespionage briefings given? Date of last briefing_____.	_____	_____
16. Are personnel aware of the requirement for foreign travel briefings and are briefings given?	_____	_____
17. Have all personnel with NATO access been briefed as required?	_____	_____
18. Do procedures ensure the Security Termination Statement is executed when required?	_____	_____

	YES	NO
19. Are DON military and civilian personnel made aware that they are subject to administrative sanctions for knowingly, willfully or negligently committing security violations?	_____	_____
20. Has the command been without incidents involving possible compromise since the last inspection?	_____	_____
21. If compromise was possible, was a preliminary inquiry conducted and reported as required?	_____	_____
22. When the loss or possible compromise of classified information has occurred, is appropriate investigative and other action taken to identify the source and reason for the compromise? Is remedial action taken to ensure further compromises do not recur?	_____	_____
23. If compromise occurred, was a JAG manual investigation conducted?	_____	_____
24. Are there procedures for handling security violations which do not result in possible compromise?	_____	_____
25. Is receipt of improperly transmitted material reported to the sender?	_____	_____
26. Are counterintelligence matters reported to NIS when required?	_____	_____
27. Have all personnel been advised of the requirement to report any contact with any citizen of a designated country?	_____	_____
28. Are investigations conducted and counter-intelligence reports made to NCIS when necessary in connection with unauthorized absentees?	_____	_____

Comment:

_____

_____

_____

C. Classification Management	YES	NO
1. Is the current level of classification of information verified as practicable before derivative classification markings as applied?	_____	_____
2. Is information extracted from a classified source derivatively classified per the classification markings shown in the source?	_____	_____

Comment:

_____

_____

_____

D. Marking (	YES	NO
1. Does each document show on its face its overall classification and declassification instructions?	_____	_____

	YES	NO
2. Are derivative classification actions based upon more than one source ("multiple sources") supported through the maintenance of adequate records?	_____	_____
3. Is the classification authority properly identified on the classified by line?	_____	_____
4. Where classification is required to protect a compilation of unclassified items, are the documents concerned marked properly, including an explanation of the basis and authority for the assigned classification?	_____	_____
5. Are file folders and disks properly marked to ensure protection in accordance with the highest level of classified information they contain?	_____	_____
6. Does the last paragraph of electrically transmitted messages show the appropriate down-grading and classification instructions?	_____	_____
7. Are electronically transmitted messages properly marked, and are adequate records maintained to show the source of assigned derivative classification?	_____	_____
8. Are additional warning notices applied as appropriate?	_____	_____

Comment:

_____

_____

_____

E. Accounting and Control	**YES**	**NO**
1. Do procedures protect incoming mail, bulk shipments and items delivered by messenger until a determination is made whether classified information is contained therein?	_____	_____
2. Are administrative procedures established for controlling secret and confidential material?	_____	_____
3. When possible, do two people copy classified documents, to help ensure positive control and safeguarding of all copies?	_____	_____
4. Are all copies of classified documents copied for any purpose, including those incorporated in a working paper subject to the same controls prescribed for the original document?	_____	_____
5. Is specific equipment designated for the reproduction of classified material and rules and warning notices posted thereon?	_____	_____
6. Is classified information properly guarded or stored in approved security containers?	_____	_____
7. Are restricted areas designated in buildings or areas where classified information is used or stored to protect the classified information?	_____	_____

	YES	NO
8. Are personnel warned specifically about the prohibitions against discussing classified information over non-secure communications circuits?	_____	_____
9. During working hours, are classified documents kept under surveillance or covered when not in use?	_____	_____
10. Are classified documents removed from storage kept under constant surveillance and face down or covered with cover sheets (Standard Forms 703, 704 or 705) when not in use?	_____	_____
11. Are carbon or plastic typewriter ribbons, carbon papers, worksheets and preliminary drafts used in the production of classified information destroyed after usage or properly safeguarded?	_____	_____
12. Has a system of security checks at the close of each working day been established to ensure that the area is secure, and are Standard Forms 701, "Activity Security Checklist," and 702, "Security Container Check Sheet," used as part of this system?	_____	_____
13. Is there an activity entry and exit program to deter unauthorized removal (and introduction) of classified material?	_____	_____
14. Are vaults or containers used for the storage of classified information or material recorded and a number of symbol affixed to each container?	_____	_____
15. Are security containers other than those listed on the National Supply Schedule, GSA, procured only with the approval of the Chief of Naval Operations (N09N)?	_____	_____
16. Is OPNAV 5510/21 maintained for each container used for storing classified material?	_____	_____
17. Do procedures provide for only cleared and trained persons to change combinations?	_____	_____
18. Are records of combinations assigned a security classification equal to the highest category of classified material authorized to be stored therein?	_____	_____
19. Are combinations to security containers classified information being followed?	_____	_____
Changed at least annually or upon change of custodian?	_____	_____
20. Is a record, i.e., Standard Form 700, "Security Container Information" maintained for each vault, secure room or container used for storing classified information?	_____	_____
21. Are damaged security containers repaired according to proper procedure?	_____	_____
22. Is classified information transmitted or transported only in accordance with specific requirements?	_____	_____

	YES	NO
23. Are appropriate receipt systems utilized?	_____	_____
24. Are the restrictions, procedures and authorization concerning escort/hand carrying of classified information being followed?	_____	_____
25. Do individuals, who are authorized to hand carry or escort classified material, receive an appropriate briefing and sign a statement acknowledging receipt of such briefing?	_____	_____
26. Is the escorting or hand carrying of classified information aboard commercial passenger aircraft approved by appropriate authority?	_____	_____
27. Does the Commanding Officer establish at least one clean-out day each year, where a portion of the work performed in every office holding classified information is devoted to the destruction of classified holdings no longer required to be held?	_____	_____
28. Is classified material stored in burn bags given adequate protection?	_____	_____
29. Are only approved devices or methods of destruction used for destruction of classified material?	_____	_____
30. Are requirements followed to ensure that all classified information intended for destruction actually is destroyed?	_____	_____
31. Are records of destruction for secret information signed by two cleared persons and maintained for 2 years?	_____	_____
32. If required, does the command have an emergency destruction plan?	_____	_____
33. Is Top Secret information reproduced without the consent of the originating activity or higher authority?	_____	_____
34. Have officials been designated to approve the reproduction of Top Secret and Secret material?	_____	_____
35. Is classified information or material transmitted or transported by approved methods?	_____	_____
36. Are visitor controls adequate to ensure that only visitors with proper clearances, need-to-know and identification are given access to classified information?	_____	_____

F. Personnel Security	**YES**	**NO**
1. Are only U.S. citizens granted access to classified information or assigned to sensitive duties?	_____	_____
2. Is U.S. citizenship verified before granting clearance?	_____	_____
3. Have all civilian positions been designated by sensitivity?	_____	_____

	YES	NO
4. Is data maintained on waivers of investigative requirements?	_____	_____
5. Is the prohibition against conducting PSIs locally being observed? (No NCIC, local police checks, etc.)	_____	_____
6. Are periodic reinvestigations initiated every 5 years for personnel holding Top Secret clearances?	_____	_____
7. Is the appropriate investigation being requested for accessor assignment including a BI for the security manager?	_____	_____
8. Is the filing of investigative reports in official personnel records strictly prohibited and such prohibition observed?	_____	_____
9. Are PSIs and personnel security determinations properly recorded on OPNAV 5520/20?	_____	_____
10. Is there a program for continuous evaluation of eligibility for access or assignment to sensitive duties?	_____	_____
11. Are adverse personnel security determination procedures being strictly observed?	_____	_____
12. Is OPNAV 5520/20 completed correctly and maintained on each cleared person or individual assigned to a sensitive position?	_____	_____
13. Are copies of OPNAV 5520/20 sent to NMPC or CMC whenever a completed PSI or security determination is entered for a Navy or Marine Corps military member?	_____	_____
14. Is access to NATO classified information being granted only after final clearance is granted and the person is briefed?	_____	_____
15. Are denials or revocation of clearances processed as required?	_____	_____
16. Is access granted only to those with a need to know and is it recorded?	_____	_____
17. Are personnel granted a security clearance prohibited from access to classified information until they have received an initial security briefing?	_____	_____
18. Has emergency access been granted and recorded for reporting purposes?	_____	_____

G. Physical Security (Ref (c) refers)	YES	NO
1. Is a Security Officer appointed in writing?	_____	_____
2. Has a Physical Security Review Committee been established?	_____	_____
3. Does the Physical Security Review Committee meet quarterly?	_____	_____
4. Are formal minutes recorded and available for review? (must be)	_____	_____

	YES	NO
5. Does the activity have a current Security Plan and does it contain the following?		
a. Identification of real property and structures to be protected?	_____	_____
b. Identify restricted and non-restricted areas?	_____	_____
c. Detail of personnel identification and access control?	_____	_____
d. Identification of physical security procedures and equipment that will detect and/or prevent wrongful removal, damage, destruction or compromise of protected property?	_____	_____
6. Does the Security Plan implement the Security Plan of the host command and does it include command Loss Prevention Plan?	_____	_____
7. Have areas been designated as Level I, II or III restricted areas as necessary to safeguard information property?	_____	_____
Have signs been posted to indicate areas as restricted?	_____	_____
8. Are the basic security measures for restricted areas listed in reference (c) in effect?	_____	_____
9. Has a key and lock custodian been appointed in writing?	_____	_____
10. Does the key and lock control program include:		
a. A key control register?	_____	_____
b. An inventory of keys with each change of custody?	_____	_____
c. Strict accountability of keys allowing access to disbursing area maintained?	_____	_____
d. Identifies by name all individuals who have been issued keys?	_____	_____
e. Date of issuance?	_____	_____
f. Date surrendered?	_____	_____
11. Does the Security Officer maintain files of approved waivers/exceptions granted for physical security discrepancies?	_____	_____
12. Is all security equipment tested at least every 6 months for proper operation and records of test available?	_____	_____
13. Are combinations changed every 2 years or upon relief of accountable individual, and is a record kept?	_____	_____
14. Is the name and phone number of the individual responsible for contents of container affixed to the inside of the container?	_____	_____

	YES	NO
15. Is the unique number of the container affixed to outside of safe? (Duty station must have access to individual responsible for contents.)	_____	_____
16. Have the number of entry ways (doors, crawl spaces, windows etc.) been kept to a minimum?	_____	_____