DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 5510.10
BUMED-M4
22 Apr 2016

BUMED INSTRUCTION 5510.10

From: Chief, Bureau of Medicine and Surgery

Subj: INFORMATION SECURITY PROGRAM

Ref: (a) E.O. 13526
(b) DoD Instruction 5200.1 of 9 October 2008
(c) SECNAV M-5510.36 of 1 June 2006
(d) DoD 5400.7-R, DoD Freedom of Information Act Program, 4 September 1998
(e) Department of the Navy Foreign Disclosure Manual of 1 September 2007
(f) DoD Instruction 5230.24 of 23August 2012
(g) DoD Manual 5220.22, Volume 3, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence, 17 April 2014
(h) SECNAVINST 5510.30B
(i) DoD Instruction 5200.01 of 9 September 2014
(j) 5 U.S.C. §552

Encl: (1) Information Security Program Manual

1. Purpose

a. This instruction establishes the Bureau of Medicine and Surgery (BUMED) Information Security Program (ISP). Enclosure (1) is the BUMED ISP Manual. The ISP applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission, and destruction of classified information. This instruction also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this instruction to describe classified material in any matter, document, product, or substance on or in which classified information is recorded or embodied, to include classified information, which resides on classified information technology (IT) systems. The term "classified," also refers to controlled unclassified information (CUI). The unauthorized disclosures of both classified and CUI could result in damage to the Department of Defense (DoD).

b. It implements the ISP within BUMED per references (a) through (j).

c. Throughout this instruction, the term, "commanding officer (CO)," includes officer-in-charge.

2. Scope. This instruction applies to all personnel, military, and civilians assigned to or employed by any element in the Budget Submitting Office (BSO) 18 and includes cleared

contractor visitors working under the purview of a CO. Personnel are individually responsible for compliance. This instruction establishes the minimum standards for classifying, safeguarding, transmitting, and destroying classified information as required by higher authority.

a. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this policy manual.

b. Civilian employees are subject to criminal penalties under applicable Federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this policy manual.

3. Records. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV M-5210.1 of January 2012.

4. Reports. The reports required in this instruction, are exempt from reports control per SECNAV M-5214.1 of December 2005, part IV, paragraph 7k.

5. Forms

a. The following Standard Forms are available electronically from the U.S. General Services Administration Web site at: http://www.gsa.gov/portal/forms/type/SF.

(1) SF 700 (04/2001), Security Container Information

(2) SF 701 (11-2010), Activity Security Checklist

(3) SF 702 (11/2010), Security Container Check Sheet

(4) SF 703 (08/1985), Cover Sheet - Top Secret

(5) SF 704 (08/1985), Cover Sheet - Secret

(6) SF 705 (08/1985), Cover Sheet - Confidential

b. The following DD forms are available at: http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

(1) DD Form 254 (Dec 1999), Department of Defense Contract Security Classification Specification

(2) DD Form 2501 (Dec 1999), Courier Authorization

c. The following OPNAV Forms are available electronically from the Department of the Navy Web site at: http://www.secnav.navy.mil/dusnp/Security/Forms/Forms/AllItems.aspx.

(1) OPNAV 5511/10 (06-2008), Record of Receipt

(2) OPNAV 5500/13 (Nov 2008), Electronic Spillage Action Form

TERRY J. MOULTON
Acting

Distribution is electronic only via the Navy Medicine Web site at:
http://www.med.navy.mil/directives/Pages/default.aspx

BUMEDINST 5510.10
22 Apr 2016

INFORMATION SECURITY PROGRAM MANUAL

Enclosure (1)

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1. Basic Policy. The BUMED Information Security Policy (ISP) establishes uniform policies for classifying, safeguarding, transmission, and destruction of classified military information (CMI) per references (a) through (g). This instruction implements BUMED's ISP within BUMED per references (b) through (g). This policy will be implemented within 180 days after receipt of this instruction.

2. Applicability and Scope

a. BUMED BSO-18 activities must establish and conduct ISP per this instruction and references (a) through (g). Any questions must be referred to the Personnel Security Manager Program Manager (BUMED-M45) via the Navy Medicine Echelon 3 Security Managers.

b. This instruction applies to all BUMED commanded activities, all military, civilian and contractor personnel, assigned to or employed by any element of BUMED, and include cleared contractor visitors working under the purview of a CO. Personnel are individually responsible for compliance. This instruction establishes the minimum standards for classifying, safeguarding, transmitting, and destroying classified information as required by higher authority.

3. Waivers and Exceptions. When conditions exist that prevent compliance with a specific safeguarding standard or costs of compliance exceed available resources, supervisors and program managers (PM) may submit a request for a waiver or exception to the requirements of these guidelines, in writing, to the host Command Security Manager (CSM). The CSM will submit the waiver, along with an endorsement to Deputy Under Secretary of the Navy, (Plans, Policy, Oversight and Integration) (DUSN PPOI) via the Navy Medicine Echelon 3 Security Managers, and BUMED-M45 for consideration and approval.

4. Roles and responsibilities

a. Chief, BUMED must:

(1) Implement, establish, administer, and oversee the ISP and issuing policy procedure per references (a) through (g);

(2) Appoint a Personnel Security Manager as the responsible manager for the implementation and oversight of the Information Security Program throughout the BUMED enterprise per references (a) through (g);

(3) Review policy biannually and ensure any interim changes are distributed accordingly to ensure widest dissemination; and

(4) Perform triennial program assessments with selected subordinate commands. This assessment can be combined with other required assessments, provided it is conducted by the subject matter expert.

b. Navy Medicine Echelon 3 commanders must:

(1) Appoint a Navy Medicine Echelon 3 Security Manager as the responsible manager for the implementation and oversight for commands within their area of responsibility per references (a) through (g) and this instruction;

(2) Develop an ISP instruction detailing their requirements to their subordinate commands; and

(3) Perform a program assessment of selected programs biannually. This assessment can be combined with other required assessments, as long as it is conducted by a subject matter expert.

c. COs must:

(1) Appoint a CSM as the responsible manager for the implementation and oversight for the command per references (a) through (g), this instruction, and the applicable Navy Medicine Echelon 3 ISP instruction;

(2) Develop a command ISP instruction incorporating BUMED and Navy Medicine Echelon 3 requirements and adding local requirements; and

(3) Complete a self-assessment annually, utilizing the check-list located in reference (c). The results of this self-assessment will be routed and signed by the CO and a copy is provided to the Navy Medicine Echelon 3 Security Manager for review. If discrepancies are identified, the command will submit a Plan of Action and Milestones (POA&M), identifying a timeline to mitigate the noted discrepancies.

CHAPTER 2
SECURITY STRUCTURE

1. Command Security Management – BSO-18 Activities Commanders and CO's. The Navy BSO-18 commanders and CO's are responsible for the effective management of the ISP within the command. Authority delegated by this policy to a CO may be further delegated unless specifically prohibited. This policy establishes baseline standards, but the CO may impose more stringent requirements within the command or upon subordinate if the situation warrants. The CO must not, separately establish requirements that impact on other commands or cleared DoD contractors, or that contradict this policy.

a. Risk Management. Commands confront different environments and sets of changing operational requirements. Therefore, each CO must apply risk management principles to determine how best to attain the required levels of protection. Employing risk management results in command decisions to adopt specific security measures given the relative costs and available resources.

b. Implementation. The CO must designate, in writing, certain security personnel directly involved in program implementation. At a minimum, the CO will designate a Security Manager and an Assistant Security Manager. Additionally, the CO must:

(1) Issue a written command security instruction per exhibit 2A.

(2) Approve an emergency plan that includes provisions for the protection and destruction of classified information in emergency situations per exhibit 2B.

(3) Establish and maintain a self-inspection program for the command. This may include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command's ISP.

(4) Establish an industrial security program when the command engages in classified procurement, or when cleared DoD contractors perform classified work or operate within areas under the direct control of the CO.

(5) Apply risk management, as appropriate, for the safeguarding of classified information, and monitor its effectiveness in the command. When assessing risk for the safeguarding of classified information, COs must give consideration to personal electronic devices that have recording, photographic, storage, or transmission capabilities and the risks associated with permitting these devices in areas where classified information is processed or stored.

(6) Ensure that the security manager and other command personnel receive training as required, and support the command security education program.

(7) Ensure that the performance rating systems of all Department of the Navy (DON) military and civilian personnel, whose duties significantly involve the creation, handling, or management of classified information, include a critical security element on which to be evaluated.

2. Navy Medicine Echelon 3 and Command Security Managers. The CSM must be designated by the CO in writing per reference (c). The CSM is responsible for implementing the ISP and must have direct access to the CO. The CSM must remain cognizant of all command information, personnel, and industrial security functions and ensures the security program is coordinated and inclusive of all requirements within the DoD, DON, and BUMED policies per reference (c). The CSM may be assigned full-time, part-time or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within 5 years prior to assignment.

a. Serve as the principal advisor and representative to the CO in matters pertaining to the classification, safeguarding, transmission, and destruction of classified information.

b. Develop a written command security instruction per exhibit 2A, to include provisions for safeguarding classified information during military operations or emergency situations.

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

d. Formulate, coordinate, and conduct the command security education program per references (c) and (i) and this instruction.

e. Ensure that threats to security and other security violations are reported, recorded, and when necessary investigated to the Navy Medicine Echelon 3 Security Manager and CSM. Ensure that incidents described in chapter 12 of this policy manual are immediately referred to the nearest Naval Criminal Investigative Service (NCIS) office.

f. Ensure that all security violations or incidents involving the possible compromise of classified information, to include those involving information technology (IT) systems, are investigated and reported to the Navy Medicine Echelon 3 Security Manager/CSM, BUMED-M45 per chapter 12 of this policy manual. Coordinate after-incident responses involving classified information processed on IT systems with the command Information Assurance Manager (IAM).

g. Coordinate the preparation and maintenance of security classification guides (SCG) under the command's cognizance.

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

i. Per reference (c), develop security measures and procedures regarding visitors who require access to classified information.

j. Per reference (c), ensure that classified information is secured and controlled areas are sanitized when a visitor is not authorized access.

k. Implement and interpret, as needed, regulations governing the disclosure of classified information to foreign governments per reference (c).

l. Ensure compliance with the requirements of this policy manual when access to classified information is provided at the command to cleared contractors in connection with a classified contract.

m. Ensure that access to classified information is limited to appropriately cleared personnel with a need-to-know per reference (b).

n. The Navy Medicine Echelon 3 Security Manager and CSM must be identified by name on command organizational charts, telephone listings, rosters, or other media. Reference (c) recommends that the security manager report to the CO on functional security matters and to the executive officer for administration of the ISP.

3. Assistant Security Manager. Persons designated as assistant security managers must be U.S. citizens, and either officers, enlisted persons E-6 or above, or civilians GS-6 or above. The designation must be made by the CO, in writing. Assistant security managers take direction from the security manager and provide support as needed. Assistant security managers must have a favorably adjudicated SSBI if they are designated to grant temporary access; otherwise, the investigative and clearance eligibility requirements will be determined by the level of access to classified information required. This position will be a required position at each BSO-18 command.

4. Security Assistant. Individuals performing administrative functions under the direction of the security manager must be a U.S. citizen and have clearance eligibility for the access required to perform their assigned duties and tasks.

5. Top Secret Control Officer (TSCO). The CO must designate, in writing, a command TSCO for commands handling Top Secret information. Top Secret Control Assistants (TSCA) may be assigned as needed. The TSCO reports directly to the security manager or the security manager may serve concurrently as the TSCO. The TSCO must be an officer, senior non-commissioned

officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI within the previous 5 years. The TSCO must:

a. Maintain a system of accountability (e.g., registry) to record the receipt, reproduction, transfer, transmission, downgrading, and declassification and destruction of command Top Secret information, less sensitive compartmented information (SCI) and other special types of classified information per reference (c).

b. Per reference (c), ensure that inventories of Top Secret information are conducted at least once annually or more frequently when circumstances warrant. As an exception, repositories, libraries, or activities that store large volumes of classified documents may limit their annual inventory to that which access has been given in the past 12 months, and 10 percent of the remaining inventory.

6. Security Education and Training Assistance (SETA) Program

a. The CSM is responsible for implementing the DON SETA. The SETA Manager must support the CSM in this endeavor. The CSM will work with the SETA Manager to ensure that security training and/or briefings are developed and presented when requested by a supervisor, PM. These presentations will be concise and address the topic requested by supervisors, PMs.

b. Supervisors, in coordination with the CSM, are responsible for determining unique security requirements and ensuring personnel under their supervision understand the security requirements for their particular assignment.

7. Other positions and collateral duties. Information related to other positions and collateral duties are listed in reference (c) as needed for specific commands.

EXHIBIT 2A

GUIDELINES FOR COMMAND SECURITY INSTRUCTIONS

1. Navy Medicine Echelon 3 Security Manager and CSM must assess the vulnerability of the command classified information to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified information, mission of the command, countermeasures available and the cost, and the effectiveness of alternative courses of action. Results of this assessment must be used to develop a command security instruction, which will emulate the organization of this policy manual and identify any unique command requirements. The command security instruction must supplement this policy manual and other directives from authorities in the command administrative and operational chain, and should be signed by the CO.

2. Per reference (c), the command security instruction must:

a. Describe the purpose, applicability, and relationship to other directives, particularly this policy manual.

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Cite and append security service agreements, if applicable.

e. Describe procedures for internal and subordinate security reviews and inspections.

f. Specify internal procedures for reporting and investigating loss, compromise, and other security discrepancies.

g. Establish procedures to report counterintelligence matters to the nearest NCIS office.

h. Establish an ISP security education program. Assign responsibilities for briefings and debriefings.

i. State whether the CO and any other command officials have been delegated original classification authority.

j. Establish procedures for the review of classified information prepared in the command to ensure correct classification and marking. Identify the sources of security classification guidance commonly used, and where they are located.

k. Establish an industrial security program and identify key personnel, such as the Contracting Officer's Representative (COR), if applicable.

l. Specify command responsibilities and controls on any special types of classified and controlled unclassified information (CUI).

m. Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.

n. Identify requirements for the safeguarding of classified information to include how classified information must be protected during working hours, stored when not in use, escorted or hand-carried in and out of the command, and protected while in a travel status. Other elements of command security which may be included are key and lock control, safe and door combination changes, location of records of security container combinations, procedures for emergency access to locked security containers, protecting telephone conversations, conducting classified meetings, safeguarding of U.S. classified information located in foreign countries, identifying IT systems processing classified information, and describing any authorized residential storage arrangements.

o. Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command emergency destruction plan, as a supplement, when required.

p. Establish command visitor control procedures to accommodate visits to the command involving access to, or disclosure of, classified information. Identify procedures to include verification of personnel security clearances and need-to-know.

3. Refer to reference (h) for guidance concerning personnel security investigations, adjudications, and clearances.

EXHIBIT 2B

EMERGENCY PLAN AND EMERGENCY DESTRUCTION SUPPLEMENT

Part One: Emergency Plan

1. COs must develop an emergency plan for the protection of classified information in case of a natural disaster or civil disturbance. This plan may be prepared in conjunction with the command's disaster preparedness plan.

2. Emergency plans provide for the protection of classified information in a way that will minimize the risk of personal injury or loss of life. For instance, plans should call for immediate personnel evacuation in the case of a fire, and not require that all classified information be properly stored prior to evacuation. A perimeter guard or controlling access to the area will provide sufficient protection without endangering personnel.

3. In developing an emergency plan, assess the command's risk posture. Consider the size and composition of the command, the amount of classified information held, situations which could result in the loss or compromise of classified information, the existing physical security measures, the location of the command and degree of control the CO exercises over security (e.g., an military treatment facility vice a leased private building), and local conditions which could erupt into emergency situations.

4. Once a command's risk posture has been assessed, it can be used to develop an emergency plan which can take advantage of a command's security strengths and better compensate for security weaknesses. At a minimum, the emergency plan must designate persons authorized to decide that an emergency situation exists and to implement emergency plans, determine the most effective use of security personnel and equipment, coordinate with local civilian law enforcement agencies and other nearby military commands for support, consider transferring classified information to more secure storage areas in the command, designate alternative safe storage areas outside the command, identify evacuation routes and destinations, arrange for packaging supplies and moving equipment, educate command personnel in emergency procedures, give security personnel and augmenting forces additional instruction on the emergency plan, establish procedures for prompt notification of appropriate authorities in the chain of command, and establish the requirement to assess the integrity of the classified information after the emergency (even though a document-by-document inventory may not be possible under current accountability guidelines).

Part Two: Emergency Destruction Supplement

1. Commands located outside the United States and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans (Electronic Key Management System Manual Series 1 (EKMS-1) provides additional

emergency destruction policy and guidance for commands that handle classified communications security ((COMSEC) information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of emergency destruction of classified information must be reported to the DUSN (PPOI) via the Navy Medicine Echelon 3 Security Manager and BUMED-M45.

2. The priorities for emergency destruction are: Priority One - Top Secret information, Priority Two - Secret information, and Priority Three - Confidential information.

3. For effective emergency destruction planning, limit the amount of classified information held at the command and if possible store less frequently used classified information at a more secure command. Consideration must be given to the transfer of the information to IT media, which will reduce the volume needed to be transferred or destroyed. Should emergency destruction be required, any reasonable means of ensuring that classified information cannot be reconstructed is authorized.

4. An emergency destruction supplement must be practical and consider the volume, level, and sensitivity of the classified information held at the command; the degree of defense the command and readily available supporting forces can provide; and proximity to hostile or potentially hostile countries and environments. More specifically, the emergency destruction supplement must delineate the procedures, methods (e.g., document shredders or weighted bags), and location of destruction; indicate the location of classified information and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified information.

5. All COs must review the emergency plan and emergency destruction plans at least annually.

CHAPTER 3
SECURITY EDUCATION

1. Basic Policy. Navy Medicine Echelon 3 commanders, activity CO's must ensure that personnel in their command receive the security education necessary to execute their security responsibilities per reference (c).

2. Responsibility. DUSN (PPOI) is responsible for policy guidance, education requirements, and support for the DON SETA program. The SETA Manager must support the CSM in this endeavor.

3. Additional Information. At a minimum, BUMED and Navy Medicine Echelon 3 Security Manager must attend the DUSN (PPOI) training symposiums. CO's should ensure their security managers attend the DUSN (PPOI) training symposiums. This allows security managers to receive the most up to date information needed to effectively manage the ISP program.

CHAPTER 4
CLASSIFICATION MANAGEMENT

1. Basic Policy

a. It is the DON policy to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information must be classified only to protect national security.

b. Per references (b) and (c), unnecessary or higher than necessary classification is prohibited. If there is reasonable doubt about the classification level of information, safeguard it at the higher level and contact the Navy Medicine Echelon 3 Security Manager for guidance.

2. Classification Levels. Information requiring protection against unauthorized disclosure in the interest of national security is classified at one of three levels.

a. Top Secret is the highest classification level. Unauthorized disclosure of Top Secret information could be reasonably expected to cause ***"exceptionally grave damage"*** to national security.

b. Secret is the second highest classification level. Unauthorized disclosure of Secret information could be reasonably expected to cause ***"serious damage"*** to national security.

c. Confidential is the third and lowest classification level. Unauthorized disclosure of Confidential information could be reasonably expected to cause ***"damage"*** to national security.

Note: No other designations must be used to identify and classify national security information.

d. CUI and/or For Official Use Only (FOUO) information is another category of information, which warrants protection in the interest of national security. CUI and/or FOUO are a designation that refers to unclassified information that does not meet the standards for classification, but is pertinent to the national interests of the United States or entities outside the Federal Government. FOUO is a designation applied to unclassified information under the reference (j), which may be exempt from mandatory release to the public.

3. Original Classification. Original classification is the "initial" decision that an item of information, if subjected to compromise, could be expected to cause damage to national security.

4. Original Classification Authority (OCA). Only OCAs who have been delegated and trained may exercise this authority and have program responsibility or cognizance over the information. This authority is not transferrable.

a. Requirements for OCA. Refer to OCA, reference (c), chapter 4 for further guidance.

b. OCA Training**.** Refer to reference (c), chapter 4 for further guidance.

c. Original Classification Criteria, Principal, and Consideration. Refer to reference (c), chapter 7 for further guidance.

d. Duration of Original Classification. Refer to reference (c), chapter 4 for further guidance.

5. Derivative Classification. Derivative Classification is the incorporating, paraphrasing, restating, or generating in new form, information that has already been classified by an OCA. Anyone who creates new material in any form using classified information is considered a derivative classifier. Derivative classifiers must observe and respect determinations made by OCAs using SCG and any other classified source documents.

a. Derivative classified data must be created and marked per reference (c), chapter 4.

b. Derivative classifiers must:

(1) Respect the original classification determinations made by the OCA.

(2) Carry forward, to any newly created documents, all pertinent classification markings.

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

6. Accountability of Classifiers. All original and/or derivative classifiers are accountable for the accuracy of their classification decisions and for applying proper classification markings. Officials with signature authority are also responsible for these decisions when exercising command signature authority.

7. Limitations on Classifying or Reclassifying. Refer to reference (c), chapter 4 for further guidance.

8. Classification Challenges. All employees in possession of classified material who, in good faith, believe that its classification level is improper are encouraged and expected to challenge the classification level of the material to the OCA and per reference (c), chapter 4.

9. Resolution of Conflicts and OCAs. Refer to reference (c), chapter 4 for further guidance.

10. Tentative Classification. Refer to reference (c), chapter 4 for further guidance.

11. Patent Secrecy Information. Refer to reference (c), chapter 4 for further guidance.

12. Independent Research and Development Information (IR&D)/Bid and Proposal. Information that is a product of contractor or individual IR&D/bid and proposal efforts, conducted without prior access to classified information and associated with the specific information in question, must not be classified unless it meets the requirements of reference (c), chapter 4.

13. Foreign Government Information (FGI). Refer to reference (c), chapter 4 for further guidance.

14. Authority to downgrade, declassify, or modify classified information. Refer to reference (c), chapter 4 for further guidance.

15. Automatic Declassification. Refer to reference (c), chapter 4 for further guidance.

16. Systematic Declassification. Refer to reference (c), chapter 4 for further guidance.

17. Mandatory Declassification Review. Refer to reference (c), chapter 4 for further guidance.

18. Information Exempt from Mandatory Declassification Review. Refer to reference (c), chapter 4 for further guidance.

19. Classified Information Transferred to the Command. All classified information officially transferred to a command in conjunction with a transfer of functions or classified information that originated in a command that has ceased to exist must become the possession of the custodial command.

20. Foreign Relation Series. Refer to reference (c), chapter 4 for further guidance.

CHAPTER 5
SECURITY CLASSIFICATION GUIDES

1. Security Classification Guides (SCG). An SCG is the primary reference source for derivative classifiers to identify the level and durations of classification for specific information elements.

a. Per reference (c), chapter 5, a SCG is a legal document that is generated to communicate a prescribed uniform system for classifying, safeguarding, and declassifying decisions set forth by OCAs for the protection of U.S. information. The information that is being protected is owned by, produced by, or for and under the control of the United States. SCGs are the primary source for derivative classifiers.

b. The OCA, having program responsibility over that information, approves the SCG in writing. SCGs are intended to facilitate proper and uniform derivative classification of information.

c. The DON has developed a computerized database providing centralized management and issuance of all DON SCGs. This program is known as the Retrieval and Analysis of Navy Classified Information program.

CHAPTER 6
CLASSIFICATION MARKINGS

1. Policy

a. Classification markings alert the staff member to the presence of classified and trigger reminders for proper handling. Reference (c) is germane for all classification procedures. They should also enable the staff member to understand exactly what is and is not classified. A properly marked document identifies the owner of the information and will indicate a date, overall markings (top & bottom), portion markings (each paragraph), source or sources of classification, declassification instructions, and any warning notices (if applicable).

b. All classified materials must be properly marked with appropriate classification markings per reference (c), chapter 6, paragraphs 6-1 through 6-35, pages 6-1 through 6-29 and Exhibit 6A through 6C, pages 6A-1 through 6C-3. You may also refer to the Marking Classified Material Job Aid for additional guidance.

CHAPTER 7
SAFEGUARDING

1. Basic Policy

a. BSO-18 staff must ensure that classified information is processed only in secure facilities, on accredited IT systems, and under conditions, which prevent unauthorized persons from gaining access per references (a) and (c).

b. BSO-18 staff must ensure that classified information is used, processed, and stored under conditions that prevent unauthorized disclosure. All CMI must be properly secured in a locked General Service Administration (GSA) approved security container, vault, modular vault, or secure room, when it is not under the direct control of a properly cleared employee with an established need to know and proper security clearance.

c. All personnel must comply with the need-to-know policy for access to classified information.

d. In addition to safeguarding classified information, personnel must ensure that CUI is safeguarded from unauthorized access by the public. Measures must be taken to protect IT systems, which store, process, and transmit such information from unauthorized access.

e. CUI and CMI is the property of the U.S. Government and not personal property. Military or civilian personnel, who resign, retire, separate from the command, or are released from active duty, must return all classified information in their possession to the applicable command from which it was received.

2. Application of Control Measures**.** All classified information will be provided a level of administrative control commensurate with its assigned classification level. This policy encompasses all classified information regardless of media.

3. Top Secret Control Measures

a. All Top Secret information originated or received by the command must be continuously accounted for, individually serialized, and entered into the command's Top Secret registry or log.

b. Top Secret information will be marked, accounted, and inventoried per reference (c), chapter 7.

4. Secret Control Measures**.** Each program must establish written standard operating procedures for safeguarding secret and confidential information. These procedures should include access control, marking, storage, transmission, and destruction requirements. All custodians are responsible for having knowledge of material in their possession.

Custodians are responsible for knowing what information is missing if a security container is left unsecured or unattended. Supervisors and PMs are highly encouraged to have custodians, within their cognizance, keep an inventory of their classified materials.

5. Confidential Control Measures. Control measures for confidential information are the same as secret information.

6. Secret and Confidential Working Papers**.** Working papers including classified notes, drafts, research papers, and similar items that are not finished documents must be marked, protected and destroyed per reference (c), chapter 7. Working papers will not be transmitted outside the command or retained more than 180 days, unless they are prepared and marked as final documents.

7. Top Secret Working Papers. The accounting, control, and marking requirements for a finished document will be followed when working papers contain Top Secret information. Contact the command TSCO for further guidance.

8. Special Types of Classified and CUI

a. Special types of classified information will be safeguarded and protected per reference (c), chapter 7.

b. CUI, FOUO, and other sensitive but unclassified information must be protected in a manner that precludes unauthorized disclosure. At a minimum, when not in use, FOUO and sensitive information must be stored inside locked desks or filing cabinets.

c. Transmission of CUI by e-mail. Unclassified e-mail containing CUI must be encrypted.

d. CUI/FOUO information may be posted on a secure Federal Information Processing (compliant with 128 bit encryption) internet Web site with access limited to U.S. Government agencies or authorized DoD contractors.

9. Alternative Compensatory Control Measures**.** Refer to reference (c), chapter 7 for further information.

10. Safeguarding Measures during Working Hours

a. Classified documents removed from storage for working purposes must have applicable cover sheets; SF 703, Cover Sheet - Top Secret, SF 704, Cover Sheet - Secret, or SF 705, Cover Sheet - Confidential, affixed to the face of the document and must be kept under constant observation and control of the authorized custodian with an established need to know.

b. Security containers and open storage areas, (hereby referred to as "security containers") must be kept under the constant visual observation and control of an authorized custodian with an established need to know when open. Security containers will be secured and locked when not in use.

c. SF 702, Security Container Check Sheet must be used to record the opening and closing of each security container. SF 702 must be conspicuously posted on each security container. When security containers have more than one drawer, a SF 702 must be posted on each drawer of the container.

d. Safeguard preliminary drafts, notes, and reproduction waste products, along with any media processing products at the highest level of classified information contained on them until they are destroyed using appropriate classified material destruction procedures.

11. End-of-Day Security Checks

a. To ensure that all classified material is properly secured, BSO-18 staff and PMs must establish procedures to conduct end-of-the day security checks in all areas where classified information is used or stored. The SF 701, Activity Security Checklist, is to be used to record these checks. These checks are appropriate for all personnel (military, civilian, and contractor) whose normal duty assignment is within a BUMED/Navy Medicine work space.

b. Additionally, the SF 702 must be utilized to record that classified vaults, secure rooms, strong rooms and security containers have been properly secured at the end of the day. Containers behind a vault door that have not been opened do not need to be checked each day. The vault door must be checked each day. The SF 701 and SF 702 must also be annotated to reflect after hours, weekend and holiday activities. These forms may be destroyed 30 days after the last entry unless they are used to support an ongoing security violation investigation. Each command must establish local processes and procedures per this instruction and reference (c), chapter 7-11.

c. Security container procedures must ensure that:

(1) After all classified material has been secured, every security container must be locked by closing each drawer or door, and rotating the dial lock to the left at least one complete turn to extend the locking bolt. Then turn the dial one complete turn to the right to ensure that it is locked.

(2) Upon completion of locking the container the employee must initial the SF 702 in the “closed by” column, indicating the time the container was closed. The same procedure must be followed for the “checked by” column. To conduct the End of Day check, first try the handle to determine if the container is actually locked. If so, indicate this in the “Checked By” column. If it is not locked, follow the procedures for reporting a security violation to the CSM.

(3) On occasion there are circumstances when no one else is around when the container is locked. In this case, it is permissible for the person locking the container to also conduct the "checked by" and initial the form. Employees initialing the SF 702 must assure that the check is completed before initialing the form.

(4) Once a staff member has assured the room, area, or building is secured, they must complete the SF 701. The SF 701 must be conspicuously posted near the exit of each room, area, or building in which classified information is used or stored.

12. Safeguarding During Visits**.** Do not discuss classified information with or in the presence of visitors, foreign nationals, workmen, or other unauthorized persons. Escorts must alert fellow workers when visitors or workmen are in the area. Take particular care to ensure you do not discuss classified information in open and public areas where unauthorized personnel could listen in.

13. Classified Meetings

a. Procedures. Classified meetings must only be held at a U.S. Government agency or a cleared DoD contractor facility with an appropriate Facility Security Clearance (FCL). For detailed information, see reference (c) chapter 7.

b. Security Sponsorship. The command can accept security sponsorship of a classified or CUI meeting at the request of a DoD contractor or an association, society, or group composed primarily of DoD personnel or DoD contractor employees, only when the subject matter is of significant interest to the command.

c. The command cannot accept security sponsorship for nongovernment association sponsored and co-sponsored meetings, without prior written approval from the Chief of Naval Operations. Forward such requests to the CSM to permit CSM concurrence and the DUSN (PPOI) approval. DUSN (PPOI) approval must be obtained before any commitments are made or any announcements are published.

d. Competencies sponsoring classified meetings are responsible for ensuring that security requirements are met and a security sponsor is appointed. Security sponsors are responsible for ensuring compliance with the requirements described in this instruction. Security sponsors must remain responsible for security requirements even though another DoD component or designated cleared contractor could undertake security administration of the meeting.

e. Competencies permitting command spaces to be used for a classified meeting but not accepting security sponsorship for the meeting must advise the command sponsoring the meeting that they are required to provide a responsible security representative and ensure necessary security measures are taken.

14. Safeguarding U.S. Classified Information in Foreign Countries. Safeguard per reference (c), chapter 7.

15. Reproduction. Reproduction of classified material and the equipment authorized for classified reproduction must be kept to the absolute minimum consistent with operational requirements. Equipment authorized for classified reproduction must also be limited and specifically designated for classified reproduction.

a. Only the TSCO may authorize the reproduction, printing, or photographing of Top Secret material.

b. Reproduction of classified material originated outside the DoD or classified documents on which there appears a reproduction or distribution restriction is prohibited without the approval of the originator.

c. Copiers intended for classified reproduction must not have an internal hard drive or be connected to any type of telecommunication lines (telephone or network). Copiers with hard drives must not be used to copy classified information without the purchase and installation of the optional data security kit.

d. Once a copier has been certified, the classification level authorized for each machine and rules for copying classified information must be posted on the machine.

e. Before permitting unclear maintenance personnel access to, or releasing classified reproduction equipment, the equipment must be inspected to ensure that no classified material has been inadvertently left behind.

CHAPTER 8
DISSEMINATION

1. Basic Policy. Classified information originated or received by DON is disseminated only within the DoD and to those activities or contractors having a need to know.

a. Classified information originated by non-DoD agencies cannot be disseminated outside the DoD without the consent of the originator.

b. Classified information can be distributed to DoD contractors provided:

(1) The information is required to fulfill a contract,

(2) The contractor has an approved FCL; and,

(3) The contractor has the required safeguarding capability. This applies, when physical possession of the material is required.

c. Distribution statements for classified and unclassified technical information will be strictly adhered to and documents cannot be distributed beyond authorized distribution statements.

2. Top Secret. Top Secret information originated with the DON must not be disseminated outside the command without the consent of the originator or higher authority and must be processed through the command TSCO.

3. Secret and Confidential. Unless specifically prohibited by the originator, Secret and Confidential information originated within the DoD may be disseminated to other DoD components and agencies within the executive branch of the U.S. Government.

4. Special Types of Classified and CUI

a. Refer to reference (c), chapter 8, paragraph 8-4; for dissemination of classified information.

b. CUI or FOUO information may be disseminated within the DoD components and between officials of the DoD components, cleared DoD contractors, consultants, and grantees in the conduct of official business for the DoD and DON provided that dissemination is not further controlled by a distribution statement. CUI or FOUO information may be released to other DoD departments and agencies of the U.S. Government as necessary in the conduct of valid official business and must be marked per reference (c), chapter 6, paragraph 6-11.

5. Disclosure of Intelligence Information**.** Refer to reference (c), chapter 8, paragraph 8-5.

6. Disclosure to Congress. Refer to reference (c), chapter 8, paragraph 8-6.

7. Distribution of Technical Documents

a. Policy. Distribution statements must be assigned to technical documents to facilitate control, secondary distribution, and release of technical documents without the need to refer requests to the originating command. Technical documents include any documentation, which tell how to do something, such as build, design, manufacture, repair, test, etc. The originating command may choose to make case-by-case exceptions to distribution limitations imposed by the statement or the originating command may assign one distribution statement to be used for all administrative, operational, or critical technology data. This is sometimes determined via the SCG. All newly generated DoD unclassified technical documents must bare one of the distribution statements described in reference (c), chapter 8, exhibit 8A; page 8A-1.

b. It is the command's policy to pursue a coordinated and comprehensive program to provide for a strong and viable military research, acquisition, and support program consistent with requirements of national security, export laws, and competitive procurement. Comply with procedures for assigning distribution statements on technical documents per reference (c), chapter 8, paragraph 8-7.

c. Originators of classified and unclassified material containing technical information must determine the extent to which the documents are available for distribution, release, and issuance without additional approvals or authorizations.

d. Technical information is described as information, including scientific information that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

e. Documents containing distribution statements will not be released beyond authorized limitations without prior approval of the originator or higher authority. This includes statements applied by contractors to proprietary technical information to which the government was given limited rights. Distribution statements remain in effect until changed or removed by the originator.

8. Public Release Review

a. It is DoD policy, per reference (c), that a security and policy review (SPR) must be performed on all official DoD information intended for public release, to include information intended for placement on publicly accessible Web sites or computer servers. Documents proposed for public release must be first reviewed at the command level per reference (e) and may be found suitable for public release without higher-level consideration.

b. Command personnel are only authorized to release information to the public that is wholly within the command mission and scope. The Public Affairs Office is responsible for ensuring that a review of material proposed for public release is completed.

c. Review time is directly proportional to the size and complexity of the material, therefore, personnel must consider the size and complexity when ensuring adequate review time. All requests should be submitted into the SPR process at a minimum of 10 business days prior to the intended release date. Review reference (e) for further information and the applicable guidelines.

CHAPTER 9
TRANSMISSION AND TRANSPORTATION

1. Basic Policy

a. The CSM must ensure that only appropriately cleared personnel or authorized carriers transmit, transport, escort, or hand-carry classified information. The transmission method should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.

b. All international transfers of classified information must be via government-to-government channels. Review reference (b), for further guidance on foreign disclosure/transfers.

c. The sender of all classified material must verify the correct mailing address. Classified material may be transmitted via the current holders GSA contractor (e.g., Federal Express) only Monday through Thursday to preclude its storage at unsecured facilities over a weekend.

d. Personnel should contact their local mail center for their hours of operation and requirements for delivery of Federal Express (FEDEX) and "Next Day" registered mail packages.

2. Transmit U.S. TOP SECRET Material. U.S. Top Secret material will only be transmitted by:

a. Direct transfer between appropriately cleared U.S. personnel;

b. The Defense Courier Service (DCS);

c. The Department of State (DoS) Diplomatic Courier Service.

d. Communications protected by a cryptographic system such as a Secure Telephone or Secure Facsimile;

e. Appropriately cleared U.S. Military, Government civilian, or Contractor personnel specifically designated as couriers.

Note: You must go through the Command's TSCO prior to any transmission of top secret material.

3. Transmit U.S. Secret Material. U.S. Secret material will only be transmitted by:

a. Any means approved for Top Secret information, except that Secret information may be introduced into the DCS only when United States control cannot otherwise be maintained;

b. United States Postal Service (USPS) registered mail within and between the United States and its territories;

c. USPS registered mail addressed to U.S. Government agencies through U.S. Army, U.S. Navy, U.S. Marine Corps, or U.S. Air Force Postal Service facilities outside the United States and its territories;

d. USPS and Canadian registered mail with registered mail receipt between U.S. Government and Canadian government installations in the United States and Canada;

e. USPS Express Mail sent between U.S. Government activities and cleared DoD contractors within and between the United States and its territories. Use USPS Express Mail service only when it is the most cost effective way to meet program requirements. USPS Express Mail service is strictly controlled in the DON and the official command mail control officer must approve each use. The "Waiver of Signature and Indemnity" block on the USPS Express Mail Label 11-B must not be executed under any circumstances. The use of external (street-side) Express Mail collection boxes is prohibited.

f. The current holders of the GSA contracts for overnight domestic express delivery such as Federal Express. The use of FEDEX external (street-side) collection boxes is prohibited. These services are also prohibited for weekend delivery. These carriers must not be used to transmit classified shipments to an air mobility command Army Post Office (APO) or onward channel shipment to Outside Continental United States destinations. COMSEC, NATO, and FGI must not be transmitted in this manner.

4. Transmit U.S. Confidential material only by:

a. Any means approved for U.S. Secret information;

b. USPS registered mail to and from APO or Fleet Post Office addressees located outside the United States and its territories, and when the originator is uncertain that the addressee's location is within U.S. boundaries;

c. USPS certified mail for information addressed to a cleared DoD contractor facility or non-DoD agencies;

d. USPS first class mail between DoD component locations anywhere in the United States and its territories. The outer envelope or wrapper must be endorsed: "RETURN SERVICE REQUESTED."

5. Transmission of special types of classified and CUI. Refer to reference (c), chapter 9.

6. Telephone Transmission

a. Classified telephone conversations must be permitted only over secure communication circuits. Secure telephone equipment should not be located in areas to which access cannot be controlled (cubicle environments) to ensure that the classified information is not overheard by unauthorized personnel.

b. Fortes' and secure terminal equipment cards are unclassified when separated from the secure telephone but must be stored separately from the equipment.

7. Classified Bulky Freight Shipments**.** The Mail Handling Facility will accept items up to 70 pounds. All items weighing more than 70 pounds will not be accepted into the USPS mail system. These items will be processed through Shipping and Receiving.

8. Transmission of Classified Material to a Foreign Government**.** Procedures for transmitting classified material to a foreign government are reflected in reference (c).

9. Preparation of Classified Material for Shipment

a. Prepare classified information for shipment by packaging and sealing it with paper sealing tape that will minimize the risk of accidental exposure or undetected deliberate compromise. Classified information will be packaged so that classified text is not in direct contact with the inner envelope or container. The outer wrappings must conceal all classification markings.

b. Enclose classified document(s) in two opaque, sealed envelopes or similar wrappings. When using USPS Express mail, the USPS Express mail envelope can serve as the outer wrapper.

c. Show on the inner envelope or container the address of the receiving activity, highest classification of the material enclosed (including applicable warning notices), and any other special instructions.

d. Do not place on the outer cover classification markings, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

e. When the classified material being transmitted is too large to package within an envelope, enclose it in two opaque sealed containers, such as boxes or heavy wrappings, or prepare it as follows:

f. When the classified material is an internal component of an encased item of equipment, you may consider the outside shell or body as the inner enclosure.

g. If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably encased, you may consider the outside shell or body as the inner enclosure.

h. If the classified material is an item of equipment that is not reasonably encased and the shell or body is classified, cover it with an opaque covering that will conceal all classified features. The covering must be secure enough to prevent inadvertent exposure of the item.

i. Specialized shipping containers, including closed cargo transporters, may be used. The container is then considered as the outer wrapping or cover.

10. Addressing Classified Information for Shipment

a. The outer envelope for classified material must be addressed to an official government activity or cleared DoD contractor and not to an individual.

b. This requirement is not intended to prevent use of office code numbers or such phrases in the address as "Attention: Research Department," or similar aides in expediting internal routing. If necessary, to direct classified material to the attention of an individual, indicate the identity of the intended recipient on an attention line on the inner container or on the transmittal.

c. When transmitting classified material to a DoD contractor by mail or GSA approved carrier (e.g., FEDEX) verify the contractor's storage capability and the official mailing address. Normally, contractor classified mailing addresses are street addresses; however, use of post office boxes is authorized provided it is the official classified mailing address provided by the Defense Security Service (DSS).

d. You may obtain a contractor's classified mailing address, via the DD-254, by contacting the contractor directly or by contacting the DSS at 1-888-282-7682. Alternatively, you may access the DSS Web site: https://www.dss.mil and request an account for the Industrial Security Facilities Database and verify storage capability and official mailing addresses online.

e. Mark the outer cover of classified material being transmitted by USPS First Class mail "RETURN SERVICE REQUESTED" and for mail weighing over 12 ounces mark the outer cover "First Class" or "Priority Mail" and "RETURN SERVICE REQUESTED."

f. Both the inner and outer envelope and/or container must show the complete and correct address of the recipient and the return address of the sender.

11. Receipting for U.S. Classified Information and Foreign Government Information

a. An acknowledgement of receipt is required for all Top Secret and Secret information transmitted or transported inside and outside the command and for all classified information transmitted or transported to a foreign government or its representative.

b. Use OPNAV 5511/10, Record of Receipt reference (c), chapter 9, Exhibit 9B; and attach it to the inner cover. The receipt must contain only unclassified information that clearly identifies the classified information. Retain Top Secret receipts for 5 years and Secret receipts for two years per reference (c). Failure to sign and return a receipt to the sender may result in a report of possible loss or compromise.

12. General Provisions for Escorting or Hand Carrying of Classified Information

a. Hand carrying classified materials must be accomplished when it is the only viable alternative and not as a matter of convenience. Regulations are specific for hand carrying in and around the installation, outside the installation, via surface or air travel and traveling outside of the Continental United States. Classified material may be carried within an installation without courier documentation, provided it is accomplished by cleared personnel and packaged appropriately. Preparation of classified information for dissemination is covered in chapters 8 through 10 of these guidelines.

b. The materials may be placed into one sealed envelope and a locking bag or it may be placed into two sealed envelopes. Classified materials leaving the installation must only be carried by a civilian, military, or contractor courier who has the proper documentation and has been trained on courier responsibilities. Packages must not make use of the locking bag as the outer wrapper when leaving the installation, instead the courier must use two sealed envelopes. Enclose classified information transported outside the installation in two opaque, sealed covers (e.g., envelopes, wrappings, or containers) durable enough to conceal and protect it from inadvertent exposure or tampering.

13. Authorization to Escort or Hand Carry Classified Information

a. The CSM and/or travelers supervisor/manager must ensure written authorization is provided to all individuals escorting or hand carrying classified information. This authorization may be the DD Form 2501, Courier Authorization Card, stated on official travel orders, or a courier authorization letter. Any of these three written authorizations may be used to identify appropriately cleared military and civilian personnel approved to escort or hand carry classified information (Special Access Programs are excluded) outside the installation. Issuance of the DD-2501 is subject to the following conditions**:**

(1) The individual has a recurrent need to escort or hand carry classified information.

(2) The expiration date may not exceed 2 years from the issue date.

(3) The written authorization must be retrieved upon an individual's transfer, termination of employment, or when authorization is no longer required.

(4) The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to hand carry classified information aboard a U.S. military aircraft.

b. All command employees authorized to hand carry classified material, on or off the installation, must take every precaution to prevent the unauthorized disclosure of the material. Employees authorized to hand carry classified information are individually responsible for protecting and safeguarding the material in their possession.

c. Hand carrying Classified Information on the Installation

(1) When classified material is hand carried as part of normal duties, employees must use a cover sheet, document folder, or an envelope to protect against casual observations. These precautions are required when moving between offices, between buildings, or through public areas.

(2) If the movement requires transportation other than walking, double wrap the material. A briefcase, mail pouch, or similar container may be considered the outer wrapping. Seal and properly address the inner wrapping.

(3) If using paper envelopes as both the inner and outer wrapper provide two secure layers of protection. If using an envelope, the inner wrapper must be clearly marked with all appropriate classifications and warning notices, properly addressed (to and from) and properly sealed with asphalt tape. "Do not use masking tape or scotch tape to seal classified packages."

(4) If using a locking bag or briefcase as the outer wrapper, there is no requirement to double wrap. The material may be placed directly in the locked bag or briefcase. Remove the keys from the bag.

d. Hand Carrying Classified Material off the Installation. Before an individual is authorized to hand carry classified material off the installation, the individual must be given a "Courier Briefing" by the command Information Security Division and issued a Courier Authorization, (Courier Card) DD-2501, Courier Authorization letter or stated on official travel orders.

e. For classified material being hand carried inside the installation:

(1) Employees may use the Base Taxi, if available, in and around the installation; to hand carry properly wrapped classified material.

(2) Employees may use privately owned or government owned vehicles to hand carry classified material.

(3) Prepare classified material to be hand carried inside the installation per paragraph 4 above.

(4) Classified material being hand carried outside the installation:

f. Persons authorized to hand carry classified material outside the installation must ensure that the proper form has been properly prepared and is enclosed in the inner envelope of the package. This is required any time you are transferring custody of classified information. Additionally, the courier must ensure that a copy is retained on-station. The office authorizing the hand carrying of classified material is responsible for ensuring the form is properly prepared and retained.

g. Deliver classified material being hand carried to a contractor facility only to the contractor's mailroom or the contractor Facility Security Officer.

h. Prepare classified material to be hand carried outside the command per paragraph 5, above. Because of the inherent security risk, hand carrying is discouraged and only approved as a last resort. Only the commander of the MTF or facility may authorize hand carrying classified material outside the Continental United States. Hand carrying classified material may only be authorized when the classified material cannot be sent by mail, secure facsimile, or other authorized means because of time constraints.

i. Authorization letter for escorting or hand carrying classified information aboard commercial passenger airlines.

j. Personnel hand carrying classified information aboard commercial aircraft must arrange advance coordination with the airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this regulation and Federal Aviation Administration (FAA) guidance. This will facilitate the courier's processing through airline ticketing, screening, and boarding procedures. Local FAA field offices can often be of assistance.

k. Classified documents being hand carried must have no metal bindings (to avoid airport metal detection) and must be double wrapped. In this circumstance, a briefcase or other luggage cannot be considered the outer container.

(1) If the classified material being transported is sealed or in packaged containers and because of size, weight, or other physical characteristics, is not suitable for packaging in envelope or boxes, the authorized courier must contact the appropriate air carrier in advance of the situation.

(2) Upon arrival at the terminal, travelers must report to the airline ticket counter before boarding and present travel documentation and the classified packages to be exempt from screening. The screening official is permitted to inspect the package for flexing, feel, weight, etc., without opening the package. Opening or reading the classified material by the screening official is prohibited.

(3) The airline representative will review documentation and package and take action to confirm the status of the traveler and package.

(4) If the airline representative is satisfied with the documentation, they will provide an escort to the screening station and advise that the package is exempt from screening.

(5) If the airline representative is not satisfied with the documentation, you will not be permitted to board the aircraft. Persons denied boarding must immediately notify their supervisor. If necessary, inform the airline screening agent that the NCIS or the Federal Bureau of Investigation agents can review the material to satisfy the screening official's concerns.

(6) If the material has to be loaded in the cargo bay, the representative of the air carrier will supervise the actual loading of the material. However, the courier must accompany the material to keep it under escort surveillance during the loading and unloading operations. Additionally, the courier must be available to conduct surveillance at any intermediate stops where the cargo bay is to be opened.

(7) Documentation required to hand carry classified material aboard commercial passenger aircraft requires an identification card that includes a photograph.

CHAPTER 10
STORAGE AND DESTRUCTION

1. Basic Policy. Classified information will be stored in a manner that will deter, detect, or delay unauthorized access. Areas in which classified information is used or stored will be limited to the maximum extent possible and will be the responsibility of the CSM.

a. Weapons or highly pilfer-able items, such as money, jewels, precious metals, or narcotics will not be stored in the same security containers as classified information.

b. External markings revealing the classification level of the information being stored in a container is prohibited.

c. Classified material, not under the personal control or visual observation of an appropriately cleared person with an established need to know, must be stored in a locked GSA approved security container, vault, modular vault, or secure room, approved for open storage.

2. Standards for Storage Equipment. Refer to reference (c), chapter 10, paragraph 10-2; page 10-1.

3. Storage Requirements. Store classified material in a GSA-approved security container, Class A or B vault, or a secure room. When a secure room is used, the physical barriers must be adequate to prevent surreptitious removal or observation of classified material.

a. Storage requirements for information based on classification level are found in reference (c), chapter 10, paragraph 10-3.

b. Additionally, the physical barriers must be able to show physical evidence of any successful or attempted forced entry. Refer to reference (c), chapter 10, exhibit 10A; page 10A-1 for secure room construction standards.

4. Procurement of New Storage Equipment. Refer to reference (c), chapter 10, paragraph 10-4.

5. Removal of Security Containers. All command custodians will ensure that all classified and unclassified material has been removed from all containers that have been used to store classified material before transport or disposal. Remove drawers to ensure no classified material has fallen behind or down the sides of the drawers.

6. Shipboard Containers and Filing Cabinets. Refer to reference (c), chapter 10, paragraph 10-6.

7. Vaults and Secure Rooms

a. Vaults and secure rooms are used to meet storage requirements for large amounts of classified material, large bulky items, or unattended computer processing of classified information. Careful consideration should be given to the need for such areas since less expensive temporary protective measures could be more practical.

b. Refer to reference (b), for further guidance on secure rooms/vaults.

8. Specialized Security Containers. Refer to reference (c), chapter 10, paragraph 10-8.

9. Decertified security containers. Security containers manufactured by Remington Rand must be removed from service and all two and four-drawer Class 5 security containers manufactured by Art Metal Products, Inc., are no longer approved for the storage of classified information. All GSA labels must be removed from decertified containers.

10. Residential Storage. Refer to reference (c), chapter 10, paragraph 10-10.

11. Replacement of combination locks. Refer to reference (c), chapter 10, paragraph 10-11.

12. Security Containers

a. GSA sets the specifications for security containers used for protecting classified material. All containers must meet GSA specifications.

b. All GSA-approved security containers have a label affixed to the face of the top drawer of the container and a second label, the text certification, affixed to the inside of the control drawer (multi-lock containers have the second label on the inside of the first drawer). A container must have both of these labels to be GSA-approved. If a container is missing either of these labels, it is not GSA-approved and must be certified.

c. Currently, the only approved combination locks are the Mas-Hamilton X-07, X-08, or X-09 (series). All security containers purchased after January 1992 will come equipped with the Mas-Hamilton X-07 (series). The Sergeant and Greenleaf (S&G) combination lock remains GSA-approved; however, purchasing a GSA-approved container with the S&G lock is prohibited. If an S&G lock or any other type of combination lock malfunctions, it cannot be repaired; it must be replaced with an X-09 (series) lock.

d. Procure all new security storage equipment from the GSA Federal Supply Schedule.

13. Combinations

a. Only personnel who have been trained in the responsibility and possess the appropriate security clearance level will change combinations to security containers, vaults, and secure rooms. Combinations will be changed when first placed in use, when taken out of service, when

an individual knowing the combination no longer requires access (unless control measures preclude continued access) and if the combination is subjected to compromise. A combination is subjected to compromise when left open and unattended.

b. When a container is taken out of service the combination must be changed to 50-25-50; set combination padlocks to 10-20-30.

c. SF 700, Security Container Information, must be used to record the combination of all security containers and the identity of all persons to be notified when the container is found open and unattended.

d. SF 700 is a two-part form. Place Part 1 of the completed SF 700 on an interior location in security containers, vault or secure room doors. Mark Parts 2 and 2A of the SF 700 to reflect the highest classification level and any special notice applicable to the information stored therein. Store Parts 2 and 2A in a security container other than the one to which it applies. If necessary, continue the listing of persons having knowledge of the combination on a separate sheet attached to Part 2.

e. With current budget constraints, multi-lock containers (one lock per drawer) are becoming a viable option for classified storage. For the purposes of posting the SF 700 and affixing open and closed signs, each drawer is considered a separate security container. Ensure all drawers are secured when not under physical control or direct visual observation.

14. Securing Security Containers. When securing security containers, rotate the dial of mechanical combination locks at least four complete turns in the same direction, and then check each drawer on the container. Rotate the dial of the XO Series locks at least one turn in each direction. If the dial is given only a quick twist, it is possible to open most locks merely by turning the dial back to its opening position.

15. Electronic Security Systems. Refer to reference (c), chapter 10, paragraph 10-16.

16. Destruction of Classified Material. Classified information must be destroyed when no longer needed. This reduces the chance for loss or compromise and frees up storage space. An annual clean out day is an excellent opportunity to reduce holdings.

17. Destruction Procedures

a. If you desire to purchase shredders approved for classified destruction, the National Security Agency (NSA) Evaluated Products List (EPL) contains a listing of high security crosscut paper shredders that have been evaluated by the NSA to meet the performance requirements of NSA/Constant Surveillance Service (CSS) Specification 02-01, High Security Crosscut Paper Shredders. The EPL may be found at: http://www.nsa.gov/ia/_files/government/mdg/nsa_css-epl-02-01.pdf, or contact the CSM for additional information.

b. All Top Secret material must be returned to the applicable TSCO for destruction. Destruction of North Atlantic Treaty Organization information must be coordinated with the CSM.

c. Secret and Confidential material may be destroyed by an NSA approved cross-cut shredder within the workspace of the custodian. Secret and Confidential material including classified scrap, waste, and working papers do not require a destruction record. Cross-cut shredding of Secret and Confidential material will be performed in a manner that reduces the information to shreds no greater than five square millimeters. Only cross-cut shredders currently listed on the NSA and CSS EPL for High Security Cross-cut Shredders may be used to destroy classified material.

d. Another method of destroying material is via regularly scheduled burn runs. More information can be found within the applicable job aid.

e. Destroy classified material that is no longer required for operational purposes, per reference (c), chapter 10.

f. Destruction of classified material will be accomplished by means that eliminate risk of recognition or reconstruction of the information.

g. Each competency is encouraged to establish an annual "clean out" day in which a portion of the workday is devoted to destroying unneeded classified information. Early disposal of unnecessary classified material can assist in reducing security costs, reducing the possibility of compromise, preparing for emergency situations, and improving protection of retained classified material.

h. Classified material transported for destruction to a location outside the custodian’s workspace must be properly secured in burn bags, boxes, or similar containers before and during transit. Until the burn bag, box, or container is actually destroyed, it must be protected, handled, and stored at the highest classification level of the material contained therein.

18. Destruction of Classified Equipment, Hardware, and Software

a. There is no single universally approved method for destroying classified equipment or hardware. The Directorate for Information Systems Security, NSA, and Classified Material Conversion (CMC) office provides technical guidance concerning appropriate methods for destruction of classified electronic media and processing equipment components.

b. As with any process dealing with classified material, there are specific shipping and delivery procedures. In addition, the CMC requires that a copy of the CMC Receipt for Destruction and a self-addressed stamped envelope must accompany all material shipments. Complete instructions for sending classified for destruction at NSA may be found at: http://www.nsa.gov/cmc/.

19. Destruction of CUI

a. CUI (e.g., FOUO, personally identifiable information), sensitive but unclassified (SBU) information, technical documents containing distribution statements B through F, must be destroyed by any means that would preclude recognition or reconstruction. This must be accomplished by cross-cut shredding.

b. IT storage media containing digital FOUO, SBU, DoD Unclassified Controlled Nuclear Information, and unclassified technical documents must, at a minimum, be reformatted prior to reuse within a DoD IT systems.

20. Disposition of classified information from the command removed from Active Status or turned over to friendly foreign governments. Refer to reference (c), chapter 10.

21. Emergency Plan and Emergency Destruction

a. Navy Medicine Echelon 3 commanders, CO's, must develop an emergency plan for the protection of classified information in case of a natural disaster or civil disturbance. This plan may be prepared in conjunction with the command's disaster preparedness plan. See exhibit 2B.

b. Emergency plans provide for the protection of classified information in a way that will minimize the risk of personal injury or loss of life. For instance, plans should call for immediate personnel evacuation in the case of a fire, and not require that all classified information be properly stored prior to evacuation. A perimeter guard or controlling access to the area will provide sufficient protection without endangering personnel.

c. In developing an emergency plan, assess the command's risk posture. Consider the size and composition of the command, the amount of classified information held, situations which could result in the loss or compromise of classified information, the existing physical security measures, the location of the command and degree of control the CO exercises over security (e.g., a ship versus a leased private building), and local conditions which could erupt into emergency situations.

d. Once a command's risk posture has been assessed, it can be used to develop an emergency plan which can take advantage of a command's security strengths and better compensate for security weaknesses. At a minimum, the emergency plan must designate persons authorized to decide that an emergency situation exists and to implement emergency plans, determine the most effective use of security personnel and equipment, coordinate with local civilian law enforcement agencies and other nearby military commands for support, consider transferring classified information to more secure storage areas in the command, designate alternative safe storage areas outside the command, identify evacuation routes and destinations, arrange for packaging supplies and moving equipment, educate command personnel in emergency procedures, give security personnel, and augmenting forces additional instruction on

the emergency plan, establish procedures for prompt notification of appropriate authorities in the chain of command, and establish the requirement to assess the integrity of the classified information after the emergency (even though a document-by-document inventory may not be possible under current accountability guidelines).

e. Commands located outside the United States and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans (EKMS-1 provides additional emergency destruction policy and guidance for commands that handle COMSEC information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of emergency destruction of classified information must be reported to DUSN (PPOI).

f. The priorities for emergency destruction are: Priority One--Top Secret information, Priority Two--Secret information, and Priority Three--Confidential information.

g. For effective emergency destruction planning, limit the amount of classified information held at the command and if possible store less frequently used classified information at a more secure command. Consideration must be given to the transfer of the information to IT media, which will reduce the volume needed to be transferred or destroyed. Should emergency destruction be required, any reasonable means of ensuring that classified information cannot be reconstructed is authorized.

h. An emergency destruction supplement must be practical and consider the volume, level, and sensitivity of the classified information held at the command; the degree of defense the command and readily available supporting forces can provide; and proximity to hostile or potentially hostile countries and environments. More specifically, the emergency destruction supplement must delineate the procedures, methods (e.g., document shredders or weighted bags), and location of destruction; indicate the location of classified information and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified information.

CHAPTER 11
INDUSTRIAL SECURITY PROGRAM

1. Basic Policy. CO's must establish an industrial security program if their command engages in classified procurement with U.S. industry, educational institutions or other cleared U.S. entities, both at the prime and sub-level, hereafter referred to as "contractors," or when cleared DoD contractors operate within areas under their direct control. Command security procedures must include appropriate guidance, consistent with reference (c) and this policy manual, to ensure that classified information released to industry is safeguarded. COs are required to develop a Program Protection Plan per reference (i) must levy these requirements on contractors via the contract.

a. COR or Technical Point of Contacts must ensure the DD Form 254, Department of Defense Contract Security Classification Specification is prepared for:

(1) Each request for proposal, request for quote or other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is provided the proper security requirements.

(2) As required during the lifetime of the contract when security requirements change.

(3) On final delivery or on termination of a classified contract.

b. The DD Form 254 will be forwarded to the appropriate COR, for review and approval.

(1) Thorough review of the Statement of Work (SOW) to determine if access to or receipt and generation of controlled unclassified and classified information is required for contract performance and identification of all security requirements in support of the scope of work.

(2) The preparation of the DD Form 254.

(3) Incorporation of any additional security requirements such as program protection plans, operations security plans, and any other Contract Data Requirements List items.

(4) Preparation of documentation required for dissemination of classified information to industry is covered in reference (c), chapter 11.

2. Authority. Refer to reference (c), chapter 11, paragraph 11-2.

3. DSS Industrial Security Mission. Refer to reference (c), chapter 11, paragraph 11-3.

4. DSS and Command Security Oversight of Cleared DoD Contractor Facilities. Refer to reference (c), chapter 11, paragraph 11-4.

5. COR for Security Responsibilities

a. Per reference (c), chapter 11, paragraph 11-5, the following industrial security responsibilities are normally assigned to the COR for Security. Other responsibilities may be required, as appropriate.

b. Review SOW to ensure that access to or receipt and generation of classified information is required for contract performance.

c. Validate security classification guidance, ensure DD Form 254 is complete, and sign the DD Form 254:

(1) Coordinate review of the DD Form 254 and classification guidance as required.

(2) Resolve problems related to classified information provided to the contractor.

d. Provide, in coordination with the PM, any additional security requirements beyond those required by reference (b) or (c), in the DD Form 254, or in the contract document itself.

e. Initiate all requests for FCL action with the DSS.

f. Verify the FCL and storage capability prior to release of classified information.

g. Validate and endorse requests submitted by industry for Limited Access Authorizations for non-U.S. citizen employees.

h. Coordinate, in conjunction with the appropriate transportation element, a suitable method of classified shipment when required.

i. Review requests by contractors for retention of classified information beyond a two-year period, and in conjunction with PMs, advise the contractor of disposition instructions or issue a final DD Form 254.

j. Ensure that timely notice of contract award is given to host commands when contractor performance is required at other locations and that a memorandum of agreements or a memorandum of understanding is in place to provide adequate security direction for the contractors.

6. Contractor Facility Security Clearances

a. Any industrial, educational, or commercial entity that requires access to classified information must be cleared by the DSS prior to gaining access to classified information.

b. Work spaces that are controlled by contractors, are considered "cleared contractor facilities." A cleared contractor facility also exists when a contractor aboard the command is furnished or furnishes a security container, vault, or secure room over which the contractor exercises security cognizance (e.g., no Government employee has the combination or access to the container). The DSS maintains security cognizance for these containers, vaults, and secure rooms. These contractors are visitors and are under the security cognizance of the host commander/CSM.

7. Personnel security clearance under the National Industrial Security Program. Refer to reference (c), chapter 11, paragraph 11-17.

8. Disclosure of Classified Information to a Contractor by Government Contractor Agencies

a. Prior to the disclosure of any classified information to a contractor facility, personnel must determine that the contractor facility has a valid FCL equal to, or higher than, the category of classified information to be disclosed. If the facility is required to have physical possession of classified material, the personnel must also determine that the facility has the DSS authorization to properly safeguard the classified information to be disclosed.

b. The DSS Industrial Security Field Operations Division maintains a database for each cleared facility which contains the FCL level and storage capability. DSS field agents update the database with any changes that adversely affect the security classification level of the FCL or storage capability to the requesting command. Inquiries must be made by letter, facsimile, or telephone. Contact the DSS at occ.facilities@dss.mil or at (1-888-282-7682) for verifications involving the storage of two cubic feet, or less, of classified information. Contractor storage capability involving the storage of over two cubic feet must be verified directly with the cleared contractor. DSS also maintains a database of cleared facilities at account.request@dsshelp.org. Cleared contractors and U.S. government employees are eligible for access to the system. Follow the instructions provided at the site to obtain access.

Note: Refer to reference (c), chapter 11, paragraph 11-4, section 4; page 11-3 for guidance on contracts awarded overseas.

9. Disclosure of CUI to a Contractor by a Government Contracting Agency

a. The SOW for unclassified efforts should provide guidance for identification and safeguarding of CUI/FOUO and technical data accessed or generated in performance of the contract.

b. CUI or FOUO information generated and/or provided under command contracts must be marked and safeguarded per reference (i).

10. Contract Security Classification Specification (DD Form 254). The purpose of the DD Form 254 is twofold: to convey security classification guidance and provide specific handling procedures to cleared contractors for classified material accessed, received and/or generated on a classified contract. A classified contract is any contract that requires access to classified information by a contractor or its employees in the performance of the contract.

11. Visits by DoD Contractor Employees

a. Classified information may be disclosed during visits provided the visitors possess appropriate Personnel Clearance Levels and have a need-to-know for the classified information. This process is championed by the CSM. The responsibility for determining need-to-know lies with the individual who discloses classified information during a visit.

b. Points of contact for contractors visiting the command will be through the CSM and will verify that visiting contractors have a FCL. Once the FCL of a contractor is established, a cleared contractor's certification of the clearance of an employee should be accepted. This certification could be by use of the visitor certification program in Joint Personnel Adjudication System. Commands must not accept a visit request hand carried by contractor personnel. Final approval of the visit is the prerogative of the CO of the command to be visited. Reference (c) addresses visit requirements for contractor employees.

c. First, contractors must be entered, approved, and scheduled by military or civilian sponsors. Secondly, all personnel require some form of base identification. This may be the Common Access Card (CAC) for those eligible.

12. Transmission or Transportation. Refer to reference (c), chapter 11, paragraph 11-12.

13. Release of Intelligence to Cleared DoD Contractors. Refer to reference (c), chapter 11, paragraph 11-13.

14. Sanitization of Intelligence. Refer to reference (c), chapter 11, paragraph 11-14.

15. Foreign Ownership, Control, or Influence. Refer to reference (c), Chapter 11, Paragraph 11-15.

CHAPTER 12
LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

1. Policy. A security violation is any knowing, willful, or negligent act which results in unauthorized disclosure of classified information. The loss or compromise of classified information presents a threat to the national security. Reports of loss or compromise ensure that incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of the loss or compromise and to remedy whatever processes or procedures may have facilitated the breech. Anyone who discovers a security violation has two responsibilities.

a. Safeguard the information or material. For instance, if it is a classified item left unattended, immediately take custody. If it is classified information transmitted via unclassified email, immediately attempt to notify all holders and have the information safeguarded.

b. Notify the CSM or a member of the commands security division.

c. Types of security violations

(1) There are two types of security violations. One results in the loss, compromise, or possible compromise of classified information. The other involves a failure to adhere to security instructions but does not result in a loss, compromise, or possible compromise.

(2) A compromise is the disclosure of classified information to an unauthorized person. An unauthorized person is any person who does not have the proper security clearance and a need-to-know. A compromise can occur knowingly, willfully, or through negligence.

(3) Compromise is possible when circumstances suggest that classified information could have been disclosed to an unauthorized person. A possible compromise occurs when classified information is left unattended, not properly stored, or not properly controlled.

(4) Loss or compromise of classified information is covered in reference (c), chapter 12, paragraph 12-8.

2. Reporting Requirements

a. When a loss, compromise or possible compromise of classified information occurs, the CSM must immediately initiate a Preliminary Inquiry (PI).

b. Information required beginning a PI:

(1) Complete identification of the information involved, including the classification level, title, media, and document control number (if any), etc.

(2) Date and time the violation was discovered.

(3) Description of the violation (e.g., security container found open and unattended, classified document missing, document found unsecured and unattended, etc.).

(4) Location of the violation (building and room number).

(5) Whether or not the information involved was secured after discovery.

c. The CSM must report all violations to the local NCIS; CO, and the DUSN (PPOI), when appropriate. The contacted NCIS office must promptly advise whether or not it will open an investigation and provide advice and assistance to the PI as necessary. Timely referral to the NCIS is imperative to ensure preservation of evidence for any possible counterintelligence.

3. PI. When a security violation occurs, a PI is conducted to determine the possibility of compromise and assess the probability of damage to national security. At the conclusion of the PI, a narrative of the findings will be prepared. This report will determine additional investigative or command actions.

4. PI Initiative

a. PIs are conducted by an individual appointed by the CSM and are conducted per reference (c), chapter 12, paragraph 12-4.

b. PI's must be initiated and completed within 10 days of the initial discovery of the incident. If circumstances exist that would delay the completion of the PI within 10 days, the next superior in the administrative chain of command, DUSN (PPOI), originator of the information, NCIS and all others identified in reference (c), chapter 12, paragraph 12-8 must be notified.

5. Contents of the PI

a. A PI is not a detailed investigation, but rather a quick examination of what happened and what classified information was involved. Upon notification, the investigating official will attempt to collect as much information about the violation as possible. In addition to collecting the information reflected in paragraph 12-2 above, investigating officials will attempt to obtain written statements from witnesses and the individual discovering the violation.

b. When the results of a PI reflect that a compromise did occur, additional investigation and reporting are required and will be initiated by the CSM. Refer to reference (c), chapter 12, paragraph 12-7.

6. Classification of the PI Message or Letter. Refer to reference (c), chapter 12, paragraph 12-6.

7. Action Taken Upon PI Conclusion

a. PIs will be forwarded per reference (c), chapter 12, paragraph 12-7.

b. Disciplinary actions will be determined by the responsible individual(s), supervisor(s), and their Total Force Consultant.

c. General guidelines and policies pertaining to discipline of civilian employees are described in reference (b). An individual's eligibility to continue to hold a security clearance will be re-evaluated when he/she fails to comply with the security procedures and is found responsible for a security violation.

8. Reporting losses or compromises or special types of classified information and equipment. Refer to reference (c), chapter 12, paragraph 12-8.

9. Manual of the Judge Advocate General (JAGMAN) Investigations. Refer to reference (c), chapter 12, paragraph 12-9.

10. JAGMAN Initiation and Appointment Letter. Refer to reference (c), chapter 12, paragraph 12-10.

11. Investigative Assistance. Refer to reference (c), chapter 12, paragraph 12-11.

12. Classification of JAGMAN Investigations. Refer to reference (c), chapter 12, paragraph 12-12.

13. Results of JAGMAN Investigations. Refer to reference (c), chapter 12, paragraph 12-13.

14. Review and Endorsement of JAGMAN Investigations by superiors. Refer to reference (c), chapter 12, paragraph 12-14.

15. Security Reviews. Classified information subjected to compromise requires a security review for classification determination. If local expertise is available, a security review must be conducted for a classification determination. If no such expertise is available, the originator or OCA of the information must be asked for a security review. A security review, however, is usually insufficient to support formal prosecution. A local reviewer must not declassify classified information. This can only be done by the OCA.

16. Classification Review. When it is determined that a compromise or loss of classified information has occurred, the CSM may request the Program Office to initiate a classification review. The PM must then coordinate a classification review of the compromised information with the cognizant OCA. (See Exhibits 12C and 12D for a sample of classification review/damage assessment format).

EXHIBIT 12A
CLASSIFICATION REVIEW/DAMAGE ASSESSMENT – SAMPLE

1. Identifying Information:

    a. SITREP Number:

    b. Program Control Number (if any):

    c. SCG:

    d. Contract Number:

2. Facts: Derived from Incident Report; enclosure (1).

3. Discussion: Weigh facts and provide outcome of classification review/damage assessment.

    a. What is the Impact?

    b. Has the PM and staff considered the impact towards the information lost or compromised?

    c. A general description of impact on effected operations and mission?

    d. Has the program identified or determined potential impact on national security?

4. Conclusion: Explain rationale for the conclusion, state impact to the program (whether slight or considerable) and determine if any Critical Program Information was affected as a result of the violation.

5. Disposition: The PM must determine if further action is required as a result of the compromise or if he/she accepts the risk and if no further action will be taken. A PM may determine course of action to modify the applicable SCGs (i.e., PM may request the Original Classification Authority to):

    a. Continue to protect the compromised information at the present level of classification.

    b. Downgrade the compromised information.

    c. Declassify the compromised information.

6. Action: If option “b” or “c” is determined applicable, the SCG for the compromised information must be modified as required per reference (c) and the Contract DD Form 254, Security Classification specification revised accordingly. All government holders of the modified information must be notified.

7. Point of Contact Information: Name, Title, Organization, Telephone Number and E-mail address.

8. Damage Assessment. This exhibit and exhibit 12B are typical samples of a Program Office classification review and damage assessment.

9. Public Media Compromise. Refer to reference (c), chapter 12, paragraph 12-18.

10. Violations and Discrepancies.

a. Discrepancies. A discrepancy exists when classified material is improperly or incompletely marked or when classified material is improperly mailed, shipped, addressed, packaged, handled, or transmitted. A discrepancy exists only when the classified material was not subjected to compromise.

b. It is considered subjected to compromise if it was:

(1) Handled by a foreign postal system when its shipping container was damaged to the extent that its contents were exposed.

(2) If the inner envelope is opened by a person who does not have a security clearance and a need to know (or a security clearance at a lower level).

(3) If it was transmitted over unsecured circuits (facsimile, telephone, Internet, Intranet, etc.).

11. Electronic Security Violations

a. An electronic spillage is defined as data placed on an information system possessing insufficient security controls to protect the data at the required classification posing a risk to national security.

b. Despite previous correspondence on this issue, there continues to be a significant number of classified ES’s across networks, degrading operational readiness and underscoring a lack of information security discipline.

c. Refer to NTD 11-08, "Electronic Spillage Requirements."

d. The OPNAV 5500/13, Electronic Spillage Action Form is used to record an electronic spillage.

12. This requirement along with applicable electronic spillage references is available on the following Web sites (Web sites are PKI/CAC enabled):

a. Electronic Spillage Center Web site: http://www.netwarcom.navy.mil/.

b. Information Security Web site: https://infosec.navy.mil/main/, once there, click on documentation, NETWARCOM, electronic spillage documents.

EXHIBIT 12B
RESULTS OF LOSS OF CLASSIFIED INFORMATION SAMPLE

5510
Date

MEMORANDUM

From: Program Manager / Competency Code
To: Command Security Manager

Subj: RESULTS OF LOSS OF CLASSIFIED INFORMATION, SITREP#

Ref: (a) Command Security Manager ltr 5510 of (date)

Encl: (1) Classification Review/Damage Assessment

l. Reference (a) requested a classification review/damage assessment to determine the impact of loss or compromise of classified information. As requested, enclosure (1) is being provided.

2. I concur with the disposition and action taken as described in enclosure (1) and will implement accordingly.

3. If you have further questions regarding this incident, please contact at (XXX)-XXX-XXXX.

// SIGNATURE//

APPENDIX A
ACRONYMS

APO	Army Post Office
B&D	Bid and Proposal
BSO	Budget Submitting Office
BUMED	Bureau of Medicine and Surgery
CAC	Common Access Card
CMC	Classified Material Conversion
CMI	Classified Military Information
CO	Commanding Officer
COMSEC	Communications Security
COR	Contracting Officer's Representative
CSM	Command Security Manager
CSS	Constant Surveillance Service
CUI	Controlled Unclassified Information
DCS	Defense Courier Service
DoD	Department of Defense
DON	Department of the Navy
DUSN (PPOI)	Deputy Under Secretary of the Navy (Plans, Policy, Oversight and Integration)
DSS	Defense Security Service
EKMS-1	Electronic Key Management System Manual Series 1
EPL	Evaluated Products List
FCL	Facility Security Clearance
FEDEX	Federal Express
FGI	Foreign Government Information
FOUO	For Official Use Only
GSA	General Services Administration
IR&D	Independent Research and Development Information
ISP	Information Security Program
IT	Information Technology
JAGMAN	Manual of the Judge Advocate General
NCIS	Naval Criminal Investigative Service
NSA	National Security Agency
OCA	Original Classification Authority
PI	Preliminary Inquiry
PM	Program Manager
SBU	Sensitive but Unclassified
SCG	Security Classification Guides
SCI	Sensitive Compartmented Information
SETA	Security Education and Training Assistance
S&G	Sergeant and Greenleaf

SOW	Statement of Work
SPR	Security and Policy Review
TSCO	Top Secret Control Officer
USPS	United States Postal Service

APPENDIX B
COMMAND SECURITY INSPECTIONS

1. Background

a. Per reference (c), each host command is required to evaluate the security posture of their Command. The Command Security Inspection Program was designed to comply with this requirement and to ensure that the procedures used within the command effectively protect national security information against unauthorized disclosure.

b. The authority to conduct command security inspections is delegated to the CSM.

2. Responsibilities

a. The CSM is responsible for the overall management of the Command Security Inspection Program and for ensuring that inspections are conducted per reference (c) and these guidelines.

b. All Navy Medicine Echelon 3/CSMs are responsible for conducting annual self-inspections, documenting and maintaining records of those self-inspections, reporting the results to the PM, BUMED-M45, who will approve plans and ensure that deficiencies are corrected.

c. Supervisors, at all levels are responsible for ensuring compliance with command security inspections and procedures. Procedures such as: ensuring the end of day security checks are conducted utilizing the SF 701 and SF 702, are used per reference (c) and these guidelines. Periodic after hours checks of office spaces are recommended.

3. Procedures

a. Before a command Security inspection, Director for Administration and the CSM will select one or more offices/areas to inspect, coordinate the inspection with the office/area supervisor, and schedule the inspection. The Information Security Team will review the following with the office/area supervisor;

(1) Previous inspection reports, if any.

(2) Records of security violations, discrepancies, and infractions, if any.

(3) Records of security briefings or security training classes presented to or taken by competency personnel.

(4) Records of end of day security checks.

(5) Records of security container combinations.

b. Ten working days after the inspection, a copy of the self-inspection report will be provided to the CSM and should include plans for correcting deficiencies found during the inspection. The CSM or the Information Security Division will be available to assist in developing necessary corrective measures to correct deficiencies noted during self-inspections.