



DEPARTMENT OF THE NAVY
NAVAL EDUCATION AND TRAINING PROFESSIONAL
DEVELOPMENT AND TECHNOLOGY CENTER
6490 SAUFLEY FIELD ROAD
PENSACOLA, FLORIDA 32508-5204

IN REPLY REFER TO

NETPDTCINST 5510.1B
N3201

MAY 10 2004

NETPDTC INSTRUCTION 5510.1B

Subj: **INFORMATION AND PERSONNEL SECURITY PROGRAM**

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) OPNAVINST 5239.1B
(d) NWP-0
(e) NCPCINST 5521.1
(f) USAN 1-69
(g) OPNAVINST 5510.100B

Encl: (1) Information and Personnel Security Manual

1. **Purpose.** To issue the Naval Education and Training Professional Development and Technology Center (NETPDTC) security organization, assign responsibilities, and depict organizational relationships.

2. **Cancellation.** NETPDTCINST 5510.1A

3. **Revision.** Since this is a major revision, marginal notations are not annotated. This instruction should be read in its entirety.

4. **Objective.** To ensure maximum uniformity and effectiveness within the command in the application of Information and Personnel Security Program policies in accordance with references (a) through (g).

5. **Scope and Responsibility.** This instruction supplements reference (a) and applies to all NETPDTC personnel (military, civilian, and contractor).

6. **Forms.** Information regarding procurement of forms used in the Information and Personnel Security Program is contained in Appendix D.


P. M. RICKETTS

Distribution: (NETPDTCINST 5216.1H)

Lists I and II

Web Access: MAIN INDEX

<https://www.netpdtc.cnet.navy.mil/index.cfm/fuseaction/directive.home/index.cfm>

MAY 10 2004

TABLE OF CONTENTS

CHAPTER 1	PROGRAM MANAGEMENT
CHAPTER 2	CLASSIFICATION MANAGEMENT
CHAPTER 3	ACCOUNTING AND CONTROL
CHAPTER 4	PERSONNEL SECURITY
CHAPTER 5	EMERGENCY PLAN
CHAPTER 6	NATO SECURITY
APPENDIX A	SECURITY CHECK AT THE END OF WORKING DAY
APPENDIX B	NETPDTC INFO & PERS SECURITY PROGRAM ORIENTATION BRIEFING
APPENDIX C	SECURITY INDOCTRINATION BRIEFING
APPENDIX D	MEDIA TRANSFER: HIGHER TO LOWER CLASSIFICATION
APPENDIX E	PROCUREMENT OF FORMS
APPENDIX F	EXTRACTS FROM THE ESPIONAGE LAWS AND FEDERAL STATUTES

MAY 10 2004

CHAPTER 1

PROGRAM MANAGEMENT1. Introduction

a. General. NETPDTC's Security Program consists of two separate but related programs:

- (1) Information and Personnel Security Program.
- (2) Physical Security and Loss Prevention Program.

b. Purpose. To provide additional policy, guidance and emphasis to reference (a) for the Navy's Information and Personnel Security Program at NETPDTC.

c. Directive Revision. The NETPDTC Security Manager has overall responsibility for revising this directive. Input will be solicited from individuals who have responsibility for portions of this directive, namely:

- (1) Information Systems Security Manager (ISSM)
- (2) Top Secret Control Officer (TSCO)

Recommendations for improvement will be submitted in writing to the Security Manager, NETPDTC (N3201), Building 803.

2. Command Security Manager. The Security Manager will be designated in writing and identified to all members of the command on organization charts, telephone listings, and rosters. The Security Manager is an Executive Officer's Assistant, reporting to the Commanding Officer on matters of security but responsible to the Executive Officer for the administration of the Information and Personnel Security Program. The Security Manager is the principle advisor and must provide guidance, coordination, and oversight necessary to ensure proper program administration. The Security Manager must be a U.S. citizen, officer, or a civilian employee GS-11 or above. The rank/grade requirements are firm. The Security Manager must have a satisfactory background investigation (BI). Duties of the Security Manager are listed in paragraphs 2-3 of reference (a) and 2-2 of reference (b).

3. Assistant Security Manager. The Assistant Security Manager works directly under the supervision of the Security Manager. Work center is room 2104 in building 2435.

MAY 10 2004

4. Top Secret Control Officer. The Naval Security Group Division Officer (N3201) will be appointed in writing as the Top Secret Control Officer and will be responsible to the Security Manager in the performance of assigned duties. Duties are defined in paragraphs 2-5 of reference (a) and 2-3 of reference (b).
5. Special Security Officer. An Intraservice Support Agreement has been executed between NETPDTC and Center for Cryptology Corry Station designating the Commanding Officer of Center for Cryptology to act as Special Security Officer for NETPDTC. The Top Secret Control Officer will serve as liaison between NETPDTC and the Special Security Officer.
6. Top Secret Control Assistant. A Top Secret Control Assistant may be assigned, as needed, to provide clerical support to the Top Secret Control Officer (TSCO). The designation will be in writing. Duties are defined in paragraphs 2-6 of reference (a) and 2-4 of reference (b).
7. Information Systems Security Manager (ISSM). The ISSM will be appointed in writing and is responsible to the Security Manager for the protection of classified information being processed in the automated system. Duties are defined in paragraphs 2-8 of reference (a), 2-2 of reference (b), and 2.3 of reference (c).
8. Naval Warfare Publication (NWP) Custodian. The NWP Custodian will be appointed in writing by the Commanding Officer, and is responsible for administration and maintenance of Naval Warfare Publications. The NWP Custodian is responsible to the Security Manager for accountability and control of classified naval warfare publications. Duties are defined in reference (d).
9. NATO Control Officer. The NATO Control Officer will be appointed in writing by the Commanding Officer, and is responsible for administration and control of NATO material. Duties are defined in reference (g). Work center is room 102 in building 803.
10. NATO Control Assistant. The NATO Control Assistant will be appointed in writing by the Commanding Officer, and is responsible to the NATO Control Officer to provide administration, control and clerical support of NATO material. Duties are defined in reference (g). Work center is (LLRC) bldg 2438.
11. Directors, Department Heads and Special Assistants
 - a. Responsible for proper safeguarding and control of

MAY 1 0 2004

classified material under their assigned areas.

b. Direct persons responsible for security of classified material within their divisions to ensure security containers under their control are properly secured prior to the end of each workday. As a minimum, the Security Container Check Sheet (Standard Form 702) will be affixed in a conspicuous location near or on all containers used for storage of classified material and will be initialed by the person who locks the container. The SF 702 will be counter-initialed by a coworker when the container is secured certifying that the container has been properly locked. Additionally, the last person leaving the working space(s) will sign Activity Security Checklist (Standard Form 701) which will be posted at the entrance to all spaces containing classified material. (NOTE: Use of the SF 701 is optional and may be used at the discretion of Department Heads.) See Appendix A for security check procedures.

12. Safeguarding Classified Information. All NETPDTC military and civilian personnel are responsible for proper safeguarding of classified information. This responsibility extends to proper handling of classified material and preventing disclosure to persons not authorized access through "loose talk" concerning assigned duties. All personnel will ensure classified material received by any means from within or outside the command is immediately delivered to the Security Manager for control.

13. Security Education and Training. The goal of security training is to develop fundamental habits of security awareness to the point that proper discretion is automatically exercised in the discharge of duties. Accordingly, security of classified material becomes a natural element of every task. Security education must be provided to all personnel whether they have access to classified information or not.

a. Security Training Responsibilities

(1) Security Manager. Maintains overall responsibility for command security training.

(2) Department Heads/Supervisors. Responsible for identifying security requirements of their organizational elements, ensuring personnel under their supervision are aware of security requirements for their particular assignments.

b. Minimum Requirements

(1) Orientation Briefings. All NETPDTC personnel will be given an orientation briefing by the Security Manager in

MAY 10 2004

accordance with paragraph 4-6 of reference (a). The briefing will be given to all newly-assigned personnel during the initial check-in process. See Appendix B.

(2) Indoctrination Briefing. Personnel requiring access to classified information will be given a security indoctrination briefing by the Security Manager prior to duty assignment involving classified access. See Appendix C.

(3) Annual Refresher Briefings. Refresher briefings will be given by the Security Manager to those having access to classified material.

(4) On-the-Job-Training (OJT). OJT will be conducted by supervisors on an "as required" basis. Supervisors must ensure subordinates know security requirements impacting on the performance of their duties.

(5) Debriefings. The Security Manager's office will debrief persons who have had access to classified material prior to termination of active duty or civilian employment or temporary separation for 60 days or more, when security clearance is administratively withdrawn, or when security clearance is revoked for cause.

(6) Other Briefings. The Security Manager will give or coordinate other special briefings as required.

14. Security Violations and Compromises

a. Within NETPDTC Headquarters. If a classified material container is found unlocked in an unoccupied space, or if classified material is found laying out in an unoccupied space, it will be immediately reported to the Security Manager during working hours or the Command Duty Officer (CDO) after hours (the CDO should make every attempt to recall the Security Manager as per the recall listing located in Bldg. 800). The container and/or classified material will be guarded until one of these officials arrive. Upon arrival, the Security Manager or the CDO will secure the classified material and follow steps outlined in Chapter 12 of reference (b).

b. Reports of Violations and/or Compromises from other Activities. Reports will be reviewed by the Security Manager to ensure the requirements of paragraphs 12-3 through 12-9 of reference (b) have been met. Disposition of the report will be made in accordance with requirements of paragraph 12-8 of reference (b).

c. Espionage. Contacts with members of the NETPDTC command

MAY 10 2004

by anyone attempting to obtain classified information should be immediately reported to the NETPDTC Security Manager at 452-1686, or to the Naval Criminal Investigative Service (NCIS) at Center for Cryptology Corry Station, Pensacola, telephone 452-6346.

MAY 1 0 2004

CHAPTER 2

CLASSIFICATION MANAGEMENT

1. Classification. Consistent with the needs to protect national security, Department of Navy policy is to make available to the public as much information concerning its activities as possible. Therefore, information will be classified only to protect national security.

2. Derivative Classification. This command does not have original classification authority. Therefore, classified material produced by NETPDTC will be classified using the derivative classification guidelines contained in Chapter 6 of reference (a).

a. Each person accomplishing derivative classification is accountable for propriety of the classifications assigned.

b. A derivative classifier must respect original classification decisions.

c. A derivative classifier must verify the current level of classification of information.

d. A derivative classifier must ensure any newly created documents reflect the originating agency assigned dates for declassification or a notation that the information cannot be automatically declassified without approval of the originating agency.

e. Personnel reviewing material (i.e., editors) created by others in their work product chain are further responsible for ensuring the security worthiness of material under their review. These personnel should also adhere to the basic guidelines set forth above.

3. Industrial Contracts. Navy contracting authorities will use Contract Security Classification Specification (DD Form 254) to convey contractual security classification guidance to their contractors. Paragraphs 11-1 and 11-2 of reference (b) applies.

4. Declassification and Downgrading

a. Only the following officials are authorized to declassify and downgrade information classified by paragraph 4-19 of reference (b).

MAY 10 2004

(1) The Secretary of the Navy with respect to all information over which the Department of the Navy exercises final classification authority.

(2) The original classification authority.

(3) The Deputies or Chief-of-Staff to those original classification authorities listed in exhibit 4A of reference (b) for classified information in their functional areas. Refer to www.navysecurity.navy.mil/infopg.htm for current origination authorities.

b. Review of Classified Holdings. Unnecessary accumulation of classified material increases the possibility of loss, makes accountability and control difficult, poses a fire hazard, necessitates additional security containers, and causes unacceptable delay if emergency destruction becomes necessary. A systematic review for declassification of documents is not required but departments/divisions holding classified material will review records annually in the interest of reducing classified holdings. If destruction of material occurs, it will be accomplished by a person having appropriate clearance.

5. Marking

a. Basic Policy. All classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material.

b. Basic Marking Requirements. Marking requirements and the application of markings vary depending on the kind of material. Basic markings for all classified material and pertaining to derivative type are:

(1) The source of classification (e.g., source document classification guide), including its date when necessary for positive identification. If you derive classification from more than one source, use the phrase "Multiple Sources." Keep a listing of the multiple sources with the file or record copy of a document or the related or accompanying documentation for other kinds of classified material. (The listing is not distributed with the material.)

(2) The agency and office of origin.

(3) The overall classification.

MAY 1 0 2004

(4) Any downgrading action required. Section 4-8 of Reference (B) refers.

(5) In addition to the foregoing, some material may require warning notices and intelligence control markings as described in paragraphs 6-11 and 6-12 of reference (b).

(6) Exhibit 8A of reference (b) further requires all newly generated classified technical documents to be assigned distribution statement B, C, D, E or F. The distribution statement assigned to a classified document will be retained on the document after declassification or until the originating command specifically changes or removes it.

c. Removable Automated Information System and Word Processing Storage Media

(1) External Markings. Removable information storage media and devices used with Automated Information Systems (AIS), typewriters, or word processing systems must be labeled using color coded labels (Standard Forms 706, 707, 708, 709, 710 and 711) clearly indicating the classification and associated markings of the information they contain. Media and devices that store information recorded in analog or digital form and are generally mounted or removed by the users or operators include magnetic tape reels, cartridges and cassettes, removal disks, disk cartridges, disk packs and diskettes, paper reels and magnetic cards.

(2) Internal Markings. AIS systems and word processing systems will provide for internal markings that clearly show the classification and associated markings of the classified information that is produced.

d. Refer to Chapter 6 of reference (b) for additional information on the proper marking of classified material.

MAY 10 2004

CHAPTER 3

ACCOUNTING AND CONTROL

1. Introduction. For the purpose of this instruction, classified material will apply to classified correspondence, messages, publications, documents, information, and equipment used by this command. Classified material must be safeguarded to ensure only personnel appropriately cleared and having a "need to know" are authorized access. This access must be closely monitored by each department. The procedures outlined herein and in references (a) and (b) will be adhered to by all personnel receiving, transmitting, processing or storing classified material.

2. Control and Distribution. All classified material will be distributed through and controlled by the Security Manager's office. Any classified material received directly by any department or office will be delivered, unopened, to the Security Manager's office for processing. The dissemination of classified information will be limited strictly to those persons who have been cleared for access per the clearance eligibility criteria set forth in Chapter 8 of reference (a), and whose official duties require knowledge on a "need to know" basis. The Guard Mail System will not be used to transmit or distribute classified material. Telecopiers, facsimile equipment, or similar devices using unsecure telephone lines will not be used to transmit classified information.

a. Top Secret. The command Top Secret Control Officer (TSCO) is responsible for receiving, maintaining accountability registers, inventory, and distributing top secret documents. A continuous chain of receipts will be maintained for each Top Secret document.

b. Secret

(1) The Security Manager will administratively control secret material received by the command. All registered mail addressed to the Commanding Officer will be receipted for by the Security Manager. The Security Manager will be responsible for the return of secret material receipts to the originating office as per reference (b) when such is received by the command.

(2) The Security Manager's office will document all secret material received by the command.

(3) When secret material is passed to another office, a document will be signed by the recipient and retained by the

MAY 10 2004

Security Manager. Two copies of the receipt will be attached to the document for use as a destruction record when required.

(4) All secret material will be hand delivered within the command. Hand delivered classified material will be covered and guarded to protect against casual observation of the classified information. A sealed envelope, pouch, or brief case will be used if movement is between buildings. Interoffice transmission can be effected with the appropriate cover sheets only.

c. Confidential. The Security Manager's office will administratively control confidential material received by the command. Upon receipt of confidential material, The Security Manager's office will log in the material and notify the proper individual or department for pick up.

d. Working Papers. Working papers are documents and material accumulated or created while preparing finished material (i.e., rough drafts). When working papers contain classified information, the accounting and marking requirements prescribed for the classification may be modified. As a minimum, working papers will be:

(1) Dated when created.

(2) Marked on each page with the highest classification of any information they contain.

(3) Protected in accordance with the classification assigned.

(4) Destroyed by authorized means when no longer needed.

3. Inventory

a. The NWP library and Top Secret material will be inventoried annually in December, upon change of command and upon relief or transfer of holders.

b. Material classified secret and below does not require inventory. However, proper control measures must be adhered to.

c. At time of inventory, all custodians will certify by written memorandum that all items in their custody require retention.

d. All secret material which has outlived its usefulness will be destroyed in accordance with destruction procedures.

4. Disposal of Classified Material. Classified material,

MAY 10 2004

including messages, will be destroyed by the department retaining the material as soon as it is no longer required, or the retention period has otherwise expired per chapter 10 of reference (b). All classified material will be destroyed by an authorized person(s) having appropriate clearance by burning, melting, chemical decomposition, pulping, pulverizing, shredding (mulching), or mutilation sufficient to preclude recognition or reconstruction of the classified information.

a. Top Secret. Top secret material will be destroyed by the TSCO and a record of destruction maintained for five years IAW reference (b), paragraph 10-19.

b. Secret. A record of destruction is not required for secret material per paragraph 10-19 of reference (b).

c. Confidential. A record of destruction is not required for confidential material per paragraph 10-19 of reference (b).

d. Witnessing Officials. Persons witnessing the destruction of classified material will:

(1) Have a security clearance at least as high as the highest category of material being destroyed.

(2) Observe the complete destruction of classified documents or burn bags containing classified material.

(3) Check residue to determine whether destruction is complete and if reconstruction is possible.

(4) Take precautions to prevent classified material or burned portions of classified material from being carried away by wind or draft.

(5) Sign certificates of destruction for top secret material when destroyed.

(6) Safeguard burn bags containing classified material according to the classification of the material therein IAW reference (b), paragraph 10-19.

5. Reproduction of Classified Material

a. Policy. Classified material will not be reproduced without authorization of the Commanding Officer, Executive Officer, or Security Manager. The reproduction of classified material will be kept to an absolute minimum and will be strictly controlled.

MAY 10 2004

b. Designated Equipment. Any copy machine designated for use by the general population will not be used to reproduce classified material. The only copying machines that can be used to reproduce classified material are:

(1) Surface Combat and Naval Aviation/Intelligence/Information (Code N3202), Bldg. 2438

(2) Professional Library (Code N832-3), Bldg. 2438

(3) Naval Security Group Division (Code N3201/N3201), Bldg. 803

c. Measures

(1) The number of copies of documents containing classified information will be kept to a minimum to decrease the risk of compromise and reduce storage. Reproduced copies of classified documents will be afforded the same security controls as those required for original documents. Reproduced material must show the classification and other special markings which appear on the original material. All reproduced material will be double-checked and remarked when the markings are not clear.

(2) The immediate vicinity of the copying machine used will be cleared of all personnel to preclude unauthorized disclosure or compromise of the material being copied.

(3) The person copying the material will keep a strict accounting of original material, copies made, and any waste resulting from the copying process. A notation will be made on all copies of the Material Control Form (OPNAV 5216/10) to show the number of additional copies reproduced. All waste material will be retained by the person responsible and disposed of in accordance with proper disposal procedures.

(4) When reproduction by DAPS is desired the following applies:

(a) DD Form 844 must be executed.

(b) An individual must be identified as a contact point. This person must be present at the time of reproduction and immediately upon completion of a job remove the document and any waste material.

6. Safeguarding. Anyone who has possession of classified material is responsible for its safeguarding. Particularly for locking classified material in appropriate security equipment when not in use or under direct surveillance of authorized

MAY 10 2004

persons. The custodian must follow procedures which ensure unauthorized persons do not gain access to classified information by sight, sound or other means. Classified information will not be discussed with, or in the presence of, unauthorized persons. For guidance and assistance for determining stowage requirements, contact the Security Manager or Security Assistant. Chapter 10 of reference (b) pertains. The Security Manager or Security Assistant will conduct announced and unannounced inspections of security containers belonging to NETPDTC departments.

a. Approved Security Filing Containers and Locks. Only filing cabinets approved by the Federal Government as security filing containers will be procured for the storage of classified material. Containers will be selected from the National Supply Schedule of the General Services Administration (GSA) as outlined in SECNAVINST 10463.1A. Containers used to store classified material will not be modified.

b. Nonapproved Security Filing Containers and Locks

(1) All nonapproved filing cabinets used to store classified material must be replaced by GSA approved security filing cabinets.

(2) Filing cabinets will not be modified to the lockbar-padlock variety to provide a means to store classified material.

c. Classified Container Information

(1) A custodian will be assigned to each classified container. The custodian's name, home address, and telephone number must be provided to the Security Manager and also attached inside the locking drawer of the container.

(2) Security Container Information (Standard Form 700) (Part 1), Instructions to Personnel Finding Container Open, will be affixed to the inside of the container holding classified material. All records of combinations of safes and security areas, secret and below, under the cognizance of NETPDTC, Pensacola, will be recorded on Part 2A of SF-700 and sealed in Part 2, and maintained by the Security Manager.

(3) Combinations to locks and safes will be given only to personnel whose official duties demand access to the container. The combination to any classified container will be changed whenever individuals, knowing the combination no longer require access or, at a minimum, annually. See paragraph 10-12 of reference (b) for additional guidance.

(4) Custodians of classified containers will verify

MAY 10 2004

identification, clearance level and authorization of personnel before giving access to their safe(s).

(5) Security Container Check Sheet (Standard Form 702) will be maintained for each security container as outlined in Chapter 10 of reference (b).

d. Removal from Storage. Classified documents removed from storage for working purposes will be kept under constant surveillance and placed face down or covered when not in use. Cover sheets will be Standard Forms 703, 704 and 705 respectively for top secret, secret and confidential documents. Classified material will be secured in classified containers during routine absences from the work space. Under emergency conditions (i.e., fire or destructive weather conditions), classified material must be secured. If time does not permit, it will be kept in the possession of the custodian and returned to proper storage as soon as possible after the emergency is over.

e. Removal from NETPDTC

(1) Classified material will not be removed from this command without written authorization of the Commanding Officer.

(2) When authorized to remove classified material from NETPDTC (including TEMADD travel), the person authorized will deliver a list of the material with a statement of understanding of Chapter 9 of reference (b) to the Security Manager. The Security Manager will prepare necessary Courier Authorization Card or Courier letter when required. Upon return to NETPDTC, all classified material will be delivered to the Security Manager for physical inventory.

7. Transmission

a. Incoming Mail. The Security Manager's office will process all incoming registered, certified and first class mail marked "Postmaster Do Not Forward, Return to Sender" that is addressed to Commanding Officer, NETPDTC. Mail that is addressed to a specific code (i.e., N8) within NETPDTC, will either be picked up at the Post Office by that code or have delivery affected by the Administrative Services Branch (Code 011). Classified mail received in any office or division will be immediately delivered to N8323. The Security Manager is responsible for returning any receipts received with classified material, applying control sheets, and determining who will see the material. The cognizant person will be notified that classified material has been received. An individual possessing a security clearance equal to the security level of the material will review the material in the Security Manager's vault and

MAY 1 0 2004

determine disposition.

b. Outgoing Mail. With the exception of classified advancement in rate examinations and classified correspondence courses, the Security Manager is the only person authorized to mail classified material from NETPDTC and will assign serial numbers and classification markings. Personnel preparing classified correspondence should consult the Security Manager for guidance.

MAY 1 0 2004

CHAPTER 4

PERSONNEL SECURITY

1. Introduction. Military and civilian employees will check in and out with the Security Manager's office during in/out processing and when they transfer within the command due to inter/intradepartmental reassignment. Military and civilian employees will not be granted security clearances until they are actually candidates for access to classified information. Access and clearance will be considered one and the same. If, for example, an individual has the investigative background and is eligible for top secret clearance but needs only confidential access for performance of normal duties, then that individual will request a confidential clearance. Clearances will not be granted for administrative convenience or for inadvertent or casual access. The outdated practice of clearing those who may physically require access to a controlled area, regardless of whether such persons need access to classified information, will not be continued. The goal is to maintain the number of individuals with security clearances to the absolute minimum consistent with occupational necessity.

2. Security Clearance Control. To more effectively control the number of security clearances, the following steps will be taken:

a. The Security Manager's office will publish a quarterly access list for all department heads. Department heads will screen the list to ensure that the personnel listed within their department are accurate and clearance levels are the minimum required to perform assigned tasks.

b. Department Heads will justify the "need to know" for each security clearance requested.

c. The Security Manager will remove from the security clearance process those individuals who require access to classified facilities but not to classified information (casual access).

d. Department Heads will establish a policy that the continuing need for access to classified information is the condition necessary for requesting a security clearance.

3. Granting Security Clearances. Personnel security clearances will be granted on the basis of "need to know." The "need to know" is defined as "the necessity for access to, knowledge of, or possession of classified information in order to carry out official military or other governmental duties." Responsibility for determining whether a person's duties require access and

MAY 10 2004

authorization to receive classified information rests with the individual holding the classified information and not upon the prospective recipient. Personnel who require access to classified information will be appropriately cleared per Chapters 8 and 9 of reference (a) and the specific procedures listed herein. Departments will adhere to these requirements when requesting access to classified material.

a. Initial Clearance. Military personnel requiring access to classified material or information who have not had a previous clearance or have not received a prior NAC or BI as appropriate to the clearance level requested, and civilian personnel requiring a top secret security clearance, will report to the Security Manager's office to complete the proper forms.

b. Department Heads. Department Heads are responsible for determining who in their department requires access and for ensuring the loyalty, reliability, judgement, and trustworthiness of those with access to classified information. No one has a right to have access to classified information solely because of rank or position. Since it is expensive and time consuming to conduct Personnel Security Investigations, especially for high level clearances, it is recommended to use those individuals who already have the proper investigative background to fill positions requiring security clearances.

c. Requesting Clearance or Access

(1) Requests for access will be made to the Security Managers's office on a Classified Material Access Certification (NETC-GEN 5521/1). A justification memo from the department head will be attached to this form with the following information:

- (a) Name and grade of nominee.
- (b) Clearance level requested.
- (c) Job title.
- (d) Specific reason/justification for clearance level requested.

(2) The Security Manager, as delegated by the Commanding Officer, will grant interim clearances and access on an as needed basis. Interim clearance and access will be made after review of local personnel records, medical records, base police records, the execution of a Classified Information Nondisclosure Agreement (Standard Form 312) and an indoctrination briefing.

(3) Final clearances must be requested and approved by

MAY 10 2004

the Department of the Navy, Central Adjudication Facility, Washington, DC.

(4) Upon receipt of the final approval message from the Central Adjudication Facility, the message will remain on file at the Security Manager's office for future reference. In addition, a copy of the message is filed in the employees personnel file.

4. Withdrawal/Revocation of Security Clearances

a. Administrative Withdrawal. An individual's security clearance will be administratively lowered or withdrawn if there is no foreseeable need for access to classified information in connection with official duties or contractual obligations. This withdrawal action will not adversely affect the individual's future security clearance eligibility.

b. Denial or Revocation for Causes. Denial or revocation of security clearance for cause is an adverse personnel security determination as described in paragraph 7-3 of reference (a). Adverse action procedures in paragraph 7-7 of reference (a) must be followed exactly.

5. Civilian Security Clearances. Reference (e) is the Department of the Navy Civilian Personnel Security Program and prescribes standard criteria and administrative procedures governing disposition of all security cases involving civilian employees and applicants for employment in the Navy.

a. Civilian Employment. No civilian will be employed, assigned, or retained in any position if such employment, assignment, or retention is not clearly consistent with the interest of national security. Determinations of suitability or eligibility for civilian employment on any basis other than loyalty are not personnel security determinations and, therefore, are not under the purview of this instruction.

b. Position Sensitivity. Each civilian position in this command will be designated as critical-sensitive, noncritical-sensitive, or nonsensitive. The number of designated sensitive positions will be held to a minimum consistent with mission requirements. Since a position may be designated as sensitive even though no classified material is handled, an individual appointed to a sensitive position does not necessarily require a security clearance. However, the individual filling the position must have the proper investigative background for that position; If an individual has a security clearance and requires access to classified information to carry out official governmental duties, then that position must be designated as either critical-sensitive for top secret access or noncritical-sensitive for

MAY 10 2004

secret and confidential access. Department heads will determine which positions should be designated as critical-sensitive, noncritical-sensitive, or nonsensitive by following the criteria in paragraph 5-3 of reference (a) and paragraph 2-1 of reference (e). When individual position action is initiated, the Request for Personnel Action (SF-52) will include the security requirements. The Director, Human Resources Office, will follow the procedures of reference (e) prior to making appointments to sensitive positions.

6. Continuous Evaluation for Eligibility. Department heads and supervisors are responsible for the continuous evaluation of their personnel and must be alert for behavior indicating unexplained affluence, financial instability, alcohol or drug abuse, mental or emotional instability, criminal conduct, or unauthorized absence. Such behavior must be brought to the attention of the Security Manager.

7. Foreign Travel Briefings. Any individual who has PCS orders to, or plans to travel to or through, a foreign country MAY require a foreign travel or defensive briefing. Whether a briefing is required will be determined by the local NCIS office or an instruction listing designated countries. Even though a briefing may not be required individuals may request one at anytime.

8. Debriefing. A debriefing will be conducted in accordance with paragraph 4-11 of reference (a) by the Security Assistant for personnel who have had access to classified information under the following circumstances:

a. Prior to termination of active military service or civilian employment, or temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.

b. At the conclusion of the access period when a limited access authorization has been granted.

c. When a security clearance is revoked for cause.

d. When a security clearance is administratively withdrawn.

At the conclusion of the debriefing, the employee will be required to read the provisions of the Espionage Act and other criminal statutes shown in Appendix E and read the Security Termination Statement (OPNAV 5511/14) and sign it. The witness to the signature then signs the Security Termination Statement.

9. Visit Requests. Visit requests for NETPDTC personnel will be initiated by the departments concerned using a Visit Request

MAY 10 2004

(OPNAV Form 5521/27). Clearance level for visits must be consistent with the level of access currently on file for the employee. After completion of the Visit Request form, it must be hand delivered to the Security Manager's office for verification. If an employee has an inactive clearance prior to an official (TAD) visit, sufficient lead time, normally three working days, are required to complete and grant the level of clearance required based on the completed investigation contained in the employees official personnel file.

MAY 1 0 2004

CHAPTER 5

EMERGENCY PLAN

1. Definition. In extreme emergencies, such as natural disasters, civil disturbances, or enemy action, emergency destruction of classified material held by NETPDTC may be necessary.
2. Responsibility. The Naval Education and Training Command is the command responsible for declaring that an emergency condition exists. All personnel having direct responsibility for, or having access to, classified material are responsible for its protection under such condition in accordance with paragraphs 10-17 through 10-12 of reference (b).
3. Natural Disaster
 - a. Discussion. It is important that classified material holdings be protected in the event of a natural disaster. This command is vulnerable to hurricanes and tornados due to its geographical location. There are three categories of classified material holdings countable to this command: COMSEC, SCI, and CONVENTIONAL (GENSER). Buildings onboard Saufley Field where classified material is stored, are capable of withstanding the impact received from natural disasters. Removal of classified material from these buildings to another facility is not necessary or desired. Therefore, the basic response to protect classified material will be to ensure all classified material is gathered up and secured in approved security containers.
 - b. Procedure. Under no circumstances will anyone subject themselves or their subordinates to death or injury to protect classified material. Timely planning and effective application of the emergency plan can greatly reduce the circumstances which could jeopardize the safety of our personnel.
 - c. Implementation. Under normal circumstances, the Commanding Officer will order implementation of the emergency plan to protect classified material. In the event conditions prevent contact with the Commanding Officer, the Executive Officer (during working hours), or the Command Duty Officer (CDO) (during nonworking hours) will implement the emergency plan.
 - (1) Department Heads. Notify their personnel to report and standby for emergency actions.

MAY 10 2004

(2) Safe Combinations. Ensure all safe and vault combinations used for storage of classified material are up to date in the Security Manager's office.

d. Action. In the event of emergency plan implementation all classified material will be gathered and put in security containers (safes). This requires collecting classified material from desks, file baskets, burn bags, etc. Remove safe drawer inventory sheets and lock the safes. Standby for further instruction and/or secure the area and depart the building should conditions be obviously unsafe.

(1) Fire. The important factors to consider in case of fire are: safety of personnel; prevention of damage to classified material while maintaining physical security; preservation of as much classified material as possible; continuous observation of the area until reentry can be accomplished; and, ensuring that safe/drawer inventories (of accountable classified material) are annotated for the material that is added to the safe from desks, baskets, burn bags, etc. If personnel are unable to extinguish the fire, allow fire fighters to enter the spaces. Ensure the names of those entering (firemen/rescue workers/medical personnel) are obtained prior to their departure and then document the extent they were exposed to classified material. The Security Manager will then be able to have those who were, or may have been exposed to classified material, complete and sign an inadvertent disclosure oath.

(2) Accountability. A positive record of accountability must be maintained for all equipment, and classified material. Accurate information concerning the status of this material is imperative. A copy of inventory holdings must be on file at the Security Manager's office and should be updated at least annually or when changes occur.

4. Priority and Method of Destruction in Case of Civil Disturbance or Other Hostile Action.

a. Priority for emergency destruction of classified material is as follows:

- (1) First. Top Secret.
- (2) Second. Secret.
- (3) Third. Confidential.

(4) Fourth. Unclassified equipment which could be of use to the enemy together with pertinent technical, descriptive and operating instructions.

MAY 10 2004

b. Methods of Emergency Destruction are:

(1) Destroy by shredding if time permits.

(2) Remove to a location out of the building and burn.

(3) Destroy by any means, ensuring classified material cannot be reconstructed. Ideally, the destruction method will provide for early attainment of a point at which the destruction process is irreversible.

5. Process

a. Department Heads and Special Assistants will take the following action to facilitate the emergency destruction of classified material:

(1) Prepare a list containing location of all storage containers within the department/division/branch. The list should be maintained in a prominent and easily accessible location.

(2) Mark containers/equipment with the priority for emergency destruction, using paragraph 4 above as a guide.

(3) Instruct personnel in procedures to be followed in an emergency.

(4) Attach to each storage container a list of personnel responsible for destruction.

b. This plan is to be executed when adequate security cannot be afforded to classified material either by removing the material or by securing it, and the possibility of compromise is imminent. The implementing authority will be the Commanding Officer; however, in his/her absence the senior individual present in a space containing classified material is authorized to implement this plan and to deviate from established plans when circumstances warrant. The importance of beginning destruction sufficiently early to preclude loss of material cannot be over-emphasized. The effects of premature destruction are considered relatively inconsequential when measured against the possibility of compromise.

MAY 10 2004

CHAPTER 6
NATO SECURITY

1. Introduction. NATO is an acronym for the North Atlantic Treaty Organization. The security standards and procedures for handling and protecting NATO information are, in most cases, different than those for U.S. information. NATO classified and unclassified information is governed by references (f) and (g). The Commanding Officer shall designate, in writing, a command NATO Control Officer and at least one alternate to ensure that NATO security procedures are observed and that NATO information is correctly controlled and accounted for. There are no rank/rate requirements to be considered for the NATO Control Officer or Assistant collateral duty.

2. Access Authorization. Access to NATO classified information will be confined to those whose duties make such access essential. No person is entitled access solely by virtue of rank, appointment or security clearance. In each case need-to-know will be established. The NATO Control Officer may approve access to NATO SECRET and below. Access requirements:

a. Possess a final U.S. security clearance commensurate with the same level of classified information access required.

b. Read and understand the proper security regulations and the penalties prescribed by law for negligence or intentional compromise of classified information.

c. Have a "need to know".

(1) The NATO Control Officer will indoctrinate individuals on a need to know basis and have the individual sign a briefing certificate.

(2) The NATO Control Officer will keep a current record or file of individuals authorized access to NATO classified information. An access roster with all persons having access will be provided to the NATO control assistant and each office having access to NATO material. Offices will include N3201, N3202, N3203 and DAPS. An updated copy will be provided whenever a change occurs.

(3) The NATO Control Officer will debrief individuals who have had access to NATO material prior to termination of active duty or civilian employment or upon permanent change of station orders.

3. Categories of NATO Information. NATO has four levels of classifications. COSMIC Top Secret (CTS), Secret (NS),

MAY 10 2004

Confidential (NC), and Restricted (NR). The first three classifications are the same as the U.S. and are given the equivalent protection. The U.S. does not have a corresponding security classification equal to NR. NATO information classified NR shall be safeguarded in the same manner as For Official Use Only so as to prevent disclosure to non-government personnel.

a. NATO documents may be stored in the same security container as U.S. classified material, provided a file divider separates them. No indication as to the subject matter shall appear on the outside of the container.

b. NATO Restricted information may be stored in filing cabinets, desks, or other containers which are located in rooms where U.S. building security is provided during non-duty hours. Where such internal security is not available, locked buildings or rooms usually will provide adequate after-hours protection.

4. Control. All NATO classified material will be distributed through and controlled by the NATO Control Assistant (located at the LLRC). Any classified material received directly by any department or office will be delivered, unopened, to the control assistant for processing. The technical library will maintain administrative control of NC and NR material adequate to preclude unauthorized access. The dissemination of NATO information will be limited strictly to those persons who have been cleared for access. NEPTDTC will only handle NATO Confidential and below.

a. The NATO Control Assistant will coordinate semiannually (June and December) with all holders of NATO classified material to review their holdings to ensure NATO classified material is reduced to the maximum extent practicable. (SECNAVINST 5510.36 refers.)

b. NATO Confidential and NATO Restricted shall be destroyed by any means authorized for U.S. Confidential material. No record of destruction is required.

c. Combinations to security containers containing NATO classified material must be changed at least annually, upon departure of an individual with access to the combination, or if the combination has been or is suspected of having been compromised. Combinations will be held by the NATO control assistant.

5. Advancement-in-Rate (AIR) Examinations. An AIR examination that contains NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or

MAY 1 0 2004

U.S. classified information it contains. The statement, **"THIS DOCUMENT CONTAINS NATO (classification) INFORMATION"**, will be affixed to the front cover or first page, if there is no cover.

a. Examinations classified NATO Confidential and below will be transmitted under double opaque and strong cover. The inner cover will be secured and bear the marking **NATO CONFIDENTIAL**. The inner cover will be enclosed in a secure outer cover. The outer cover will bear an address and will not indicate the classification of the contents or the fact that it contains classified information. The outer envelope shall be marked, **"POSTMASTER DO NOT FORWARD. RETURN TO SENDER."**

b. NATO Confidential examinations may be sent via U.S. First Class mail between U.S. Government activities within the United States. Transmitted outside the United States and its territories shall be by U.S. Postal Service registered mail and remain in APO/FPO channels. Insured mail is not authorized.

6. Reusable Learning Objectives (RLOs)/Non Resident Training Courses (NRTC). No NATO information will be produced in an RLO, NRTC or web-based format.

7. Communication and Information Systems (CIS) and networks. Once a CIS has been accredited to process NATO classified information, the following minimum methods will be used to protect NATO information within CIS or networks:

a. All personnel given access to NATO classified information via a CIS or network must first be briefed on NATO security procedures and must have signed a briefing certificate. Personnel assigned to N3201, N3202, N3203 and DAPS must check in with the NATO Control Officer (Bldg 803) to receive their briefing.

b. NATO classified information may be placed on the same storage media and in the same folders as U.S. classified information. Access to the folders or directories will be limited to those individuals who have been given access to NATO classified information. The NATO and U.S. information in the folders or directories must be of the same functional area (e.g., logistics, intelligence, etc.). No NATO will be stored on systems unless requirements of paragraph 7.b(1) are met.

(1) Where all users within a network are NATO briefed and all have a need to know, the entire local network may function in the capacity of a folder and the system log-on will be treated as the access control mechanism. All personnel assigned to N32 who possess an EDSLOGIN password will be briefed into NATO.

MAY 10 2004

(2) In a situation where an originator has placed a distribution limitation statement on the information or a network customer wants information coming to their organization placed in a limited access folder, a tighter access control mechanism, as determined by the ISSO, will be needed.

c. Passwords and other information which control access to NATO classified information shall be protected in accordance with the highest classification of the NATO information to which they allow access.

d. NATO classified information may be e-mailed within the local area network (LAN) or between LANs that are accredited to process NATO information. It is the sender's responsibility to verify that the receiver is cleared for NATO information and has a need-to-know. It is also the sender's responsibility to ensure a network accredited to process NATO classified information hosts the receiver.

e. In addition to U.S. labeling requirements, all equipment (removable storage media, fixed hard drives and monitors) which stores, processes or displays NATO classified information, must be labeled according to the highest NATO classification stored, processed or displayed.

MAY 10 2004

APPENDIX A

SECURITY CHECK AT THE END OF THE WORKING DAY

1. Individuals will ensure their working area is free of security violations by:
 - a. Looking on top of, under, behind and in desks for classified material.
 - b. Ensuring that working trays and baskets are empty.
 - c. Properly storing or shredding notes, carbon paper, rough drafts or similar working papers that might contain classified information.
 - d. Placing classified documents, correspondence or related classified material in proper security containers.
 - e. Ensuring disks are removed from PC's.
 - f. Securely closing each drawer or door of the security container and locking the container by rotating the dial at least four complete turns in the same direction.
 - g. Checking the locking drawer to make sure the container is secured.
 - h. Signing off the Security Container Check Sheet (SF 702).
 - i. Surveying the general area to be sure no classified material is unsecured. This includes looking on top of and in between security containers, general storage cabinets, working tables and checking trash cans.
2. A double-check system using the Activity Security Checklist (SF 701), is required for departments/divisions which have a significant amount of security containers and work with classified material on a daily basis. Each week, a member is designated as being the last person to leave the space/building and assigned responsibility for double-checking the spaces to ensure they have been secured using the daily security checklist. Each item on the list will be checked and initialed. The double-checker will ensure:
 - a. All security containers in the area are closed and locked by rotating the combination dial four times in the same direction and trying the locking drawer.

~~NY~~ 10 2004

b. The reproduction machine is cleared by running it once and checking the reproduction paper for impressions. Machines will be turned off on weekends and holidays.

c. The shredder is cleared. The shred receptacle will be checked to ensure residue is from more than ten shredded pages.

d. The telecopier is cleared.

e. Security container tops are cleared.

f. Individual office spaces are cleared.

g. Desk tops and trays are cleared.

h. Typewriter ribbons are removed from machines using carbon ribbons on which classified information has been typed.

i. Any electrical appliances are disconnected.

j. The general area is surveyed.

k. If anyone is still working in the area with a security container open, he/she is listed as an exception beside the item on the checklist, which has not been secured. That person will then be responsible for securing the item, double checking, and initialing the checklist, and showing the time of securing.

3. Each individual is responsible for performing the security check assigned. It is the individual's responsibility to arrange with their supervisor for a substitute to perform the double check when absence is anticipated. In the unplanned absence of the assigned double checker, the supervisor will designate a substitute.

MAY 10 2004

APPENDIX B

**NETPDTC PENSACOLA INFORMATION AND PERSONNEL SECURITY PROGRAM
ORIENTATION BRIEFING**

1. Information and Personnel Security Program. An effective program exists within this command to safeguard against compromise of classified material and information. You are part of this program. During your stay at NETPDTC Pensacola, you may be required to participate in lectures, films, and other security awareness training. The goal of security training is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified material becomes a natural element in every task. Periodic refresher briefings are given for personnel who have been granted access.
2. Security Manager. The Security Administration Office in Building 2435, room 2104, is the location of the NETPDTC Assistant Security Manager's office. The phone number is 452-1001 x1447. Assistance is provided on request, don't hesitate to call. The Security Manager is located in Building 803, room 101. The phone number is 452-1686.
3. Personnel Security Clearances. Not every individual has access to classified material. Clearance and access will be granted depending on the requirements of the job. However, all personnel having knowledge of classified material or information are responsible for maintaining security thereof, no matter how that information was obtained.
4. Telephone Transmission. Classified information will not be discussed or "talked around" on the telephone except as authorized on approved secure telephones or communications circuits. It is not necessary to state, "This is not a secure line.", because unless the special equipment is being used, there is no reason to believe a line could be secure.
5. Foreign Travel. If you plan to travel to or through a foreign country you may require a briefing. Contact the Security Manager's office for a determination.
6. Violations. If you suspect a security violation, contact the Security Manager immediately at 452-1686. Any person discovering unprotected classified information has two immediate responsibilities: First, to attempt to protect the classified information from further compromise or risk of compromise; and second, to report the circumstances to a responsible official. During nonduty hours or during working hours in the absence of assigned personnel, the Command Duty Officer (CDO), telephone

MAY 10 2004

452-1628, will be notified.

7. Misrouted Mail. If you are in receipt of classified mail that was misrouted to your office, DO NOT TRY TO DELIVER IT TO THE PROPER ADDRESSEE YOURSELF - CONTACT THE SECURITY MANAGER'S OFFICE, BRING THE MATERIAL OVER TO BUILDING 803 AND WE WILL ENSURE THE MAIL GETS TO THE RIGHT ADDRESSEE.

8. I, _____, acknowledge that I have read and understand the above briefing _____ (date).

REMEMBER, SECURITY IS EVERYBODY'S BUSINESS!

MAY 10 2004

APPENDIX C

SECURITY INDOCTRINATION BRIEFING
TO BE READ BY EVERYONE BEING GRANTED A
SECURITY CLEARANCE AT NETPDTC

1. Commanding Officers are directly responsible for safeguarding all classified information within their commands and for ensuring classified material not in actual use of appropriately cleared personnel or under their direct personal observation is stored in the manner prescribed in Chapter 10 of SECNAVINST 5510.36, Department of the Navy Information Security Program Regulation, Navy's Information Security Manual.
2. The Security Officer is designated the Security Manager for NETPDTC Pensacola and will assist the Commanding Officer in fulfilling his/her responsibilities for the security of classified information. The Assistant Security Manager will serve as the principal assistant to the Security Manager in the development and execution of the station's classified material security program.
3. Department heads are responsible for the security of classified material within their respective departments. If an individual is appointed as a departmental security representative, the name of this individual must be provided to the Assistant Security Manager.
4. Every individual in the Department of the Navy who acquires access to classified information is responsible for protecting that information per Chapter 7 of SECNAVINST 5510.36. Clearance for access to classified matter is considered extremely important. All personnel having knowledge of classified material are responsible for maintaining security thereof, no matter how that information was obtained.
5. The determination that information requires protection is called classification. Classified information must be identified/marked with a classification. The classifications, in order of the highest security level to the lowest, are TOP SECRET, SECRET, and CONFIDENTIAL. Each classification requires specified protective measures. The loss of any classified material will result in damage to the national security.
6. Classified information may only be given to individuals who have been authorized access. Just as classified material is assigned levels of classification, there are different levels of personnel security clearances. Individuals are cleared for access to the level of information they will require in the

MAY 10 2004

performance of their job. For example, a person whose job requires access to secret material will be given a secret clearance and may have access to secret and confidential information, but not top secret. However, just because you hold a secret clearance does not mean you have access to all secret information. You must also have a "need to know;" that is, besides having the proper clearance; your official duties must require that you have the information.

7. Safeguarding requirements permit classified information to be used or stored only where and when it can be properly protected. This means that there are many things you may not do with classified information. YOU MAY NOT:

a. Leave classified information unprotected - it must either be properly stored or in the custody of a cleared person.

b. Read or discuss classified information in an unsecure area - classified information may be used only where uncleared persons or persons without a need to know will neither see nor hear it.

c. Remove classified information from the command - except in approved situations and with specific written permission of the Commanding Officer or designated official.

d. Reproduce classified information - except as approved by a designated official.

e. Give classified information to a visitor without first verifying the visitor's identification, clearance, and need to know.

f. Discuss classified information over the telephone.

g. Send classified information out of the command by other than approved methods.

h. Dispose of classified information by other than approved methods and with the required records.

i. Store security container combinations in insecure places.

j. Take classified information with you when you leave this employment - classified information is official information, not personal property.

8. You are responsible to ensure any classified material in your possession is safeguarded. A security representative has been designated within each department to advise you of specific

MAY 10 2004

procedures within your office. The following are our command requirements:

- a. During work hours, classified material on desks and in routing baskets should be placed face down when not in use.
- b. If leaving for lunch or a coffee break, classified material must either be locked up or under continuous observation by a cleared individual.
- c. Do not ask a messenger to pick up or deliver classified matter without verifying that person's clearance.
- d. Upon securing for the day, all desks are to be cleared of classified material and the material locked up.
- e. Locked desk drawers or briefcases may not be used even temporarily to safeguard classified material.
- f. Tumbler locks on safes are to be spun at least four times and drawer handles pulled to ensure the container is locked. The Security Container Check Sheet (SF-702) on top of the container should then be initialed and witnessed.

9. All personnel answering the telephone in spaces where classified or sensitive information is processed must be aware of conversations which discuss or touch on classified information-- immediately terminate conversation for a more secure means of communications (STU III). Personnel must not discuss or transmit classified information over the telephone or in such manner as to be intercepted by unauthorized persons.

10. Sometimes when the rules are not followed or somebody makes a mistake, a situation will occur in which classified information may be compromised. Any person discovering unprotected classified information or an unauthorized disclosure of classified information has two immediate responsibilities: First, to attempt to protect the classified information from compromise or risk of compromise; and second, to report the circumstances to a responsible official. If you cannot both protect the classified information and report the occurrence, have someone else make the report while you continue to protect the information. If you are ever the cause of a compromise or are approached by someone and asked to make an unauthorized disclosure of classified information, don't try to handle the situation yourself -- Report it immediately to the Security Manager at 452-1686 or your supervisor. REMEMBER, SAFEGUARDING CLASSIFIED INFORMATION IS A TEAM EFFORT. IF YOU NEED HELP --- SEEK IT.

MAY 10 2004

11. Any individual who has had access to classified information who plans to travel to or through a communist-controlled country or to attend a meeting in the United States or elsewhere in which representatives of communist-controlled countries are expected to participate, may be required to be given a defensive briefing. This briefing will be given by an NCIS agent. When the individual returns, they will be debriefed by an NCIS agent.

MAY 1 0 2004

APPENDIX D

MEDIA TRANSFER: HIGHER TO LOWER CLASSIFICATION

Record of data transfer procedures from a higher classified system to a lower classified system (including Unclassified).
"Transferring the safe and secure way"

1. These data transfer procedures facilitate the transfer of data between systems of unequal classification levels or Accredited Security Parameters. The command Information System Security Manager (ISSM) or a specifically authorized and properly trained representative are the only personnel authorized to perform these procedures.

2. These procedure facilitate the transfer of unclassified or lower classified data to magnetic media from a system with a higher classification level for subsequent transfer to an AIS operating at a lower security level.

a. Individual conducting this data transfer must:

(1) Obtain new magnetic media.

(2) Follow the transfer procedures outlined below and initial each phase of the transfer process.

(3) Notify the command ISSM of any problems, unusual circumstances, or inconsistencies that may occur during the data transfer.

(4) Sign and forward the completed form to the command ISSM.

(5) Retain a copy of this completed form for individual records.

3. Only the following file formats will be copied from a higher classification system to a lower classification system:

a. TXT-Text only format

b. RTF-Rich text format

c. HTM/HTML-Hypertext markup format

d. FIL-Formflow Data stored as ASCII comma delimited text file.

e. JPG/JPEG-File interchange format (graphics)

f. BMP-Bitmap graphics format

g. GIF-Graphical Interchange Format

4. Copying of DOC, PPT, XLS, MDB, TIF, or any other type of file not listed above is prohibited.

MAY 10 2004

5. Conversion for non-allowed file formats.

If the document is not a text or graphic file in one of the following five formats, TXT, RTF, HTM/HTML, JPG, or BMP, convert it to one of these five formats. This step is required because many proprietary document formats hide unintended information, to include contents of previous revisions, other unrelated files, and arbitrary contents of memory. This information may not be visible from within the application. Furthermore, this data may not be in text form, so that it cannot be reviewed and determined to be at the intended classification level.

6. Guidance for specific document types:

a. Microsoft Word documents: If transferring a Microsoft Word document, save it in RTF, TXT, or HTM/HTML format. WARNING: The native Microsoft Word .DOC file format has multiple security holes which allow the inadvertent inclusion of data from previous revisions, from other unrelated files, and from other data in your computer's memory. Do not transfer DOC files from a classified computer.

b. Spreadsheets and databases: Spreadsheet and database files cannot be transferred as-is. Export these documents as text, then transfer the text files only. Saving these files as ASCII delimited files will facilitate importing them to the spreadsheet or database on the lower classification system.

c. Microsoft PowerPoint documents: Microsoft PowerPoint documents consist mainly of data, which cannot be interpreted by a human reviewer. Some versions of Microsoft PowerPoint write arbitrary pieces of memory into a PowerPoint document. To avoid these risks, PowerPoint document must be saved as text, then transfer the text Outline/RTF or as HTM/HTML only. Reconstruct the PowerPoint briefing on the less-classified system.

NOTE: If saving the presentation as HTM/HTML, the graphics must be saved as JPG files.

d. Graphics files: Graphic files (JPG and BMP formats only) can be reviewed using standard image viewers and safely transferred.

e. Executable files: Executable program files are typically very long and almost entirely unintelligible. They will not be transferred. Obtain the program from unclassified sources instead.

NOTE: Programmers: Instead of transferring executables, transfer the text source code from the classified system and

~~MAY~~ 10 2004

recompile it on the less-classified system.

7. The attached transfer information sheet and checklist must be accomplished every time files are extracted from a higher classified system for transport to a lower system.

MAY 10 2004

1. TRANSFER INFORMATION:

A. Date: _____

B. Person Transferring Data: _____ 3. Phone:

C. Date last trained on this procedure: _____

2. Source System:

A. System Identification: _____

B. System Classification Level/ASP: _____

3. Target System:

A. System Identification: _____

B. System Classification Level/ASP: _____

4. Transfer Media:

A. Command Media Control Number (if used): _____

B. Media Classification Before Transfer: _____

C. Media Classification After Transfer: _____

5. Data Transferred:

A. Data Type(s): _____
(E.G. TXT, BMP, ect.)

B. File Name(s): _____

6. Transfer Procedures: (Initial each item)

_____ Obtain new magnetic media. This media MUST be new and may never have been used to store data:

MAY 10 2004

_____ If necessary, format/initialize the media on the target system or a system with the same accreditation as the target device: (format by MS DOS Format- FORMAT A: /U, using the File Manger/Windows Explorer format could leave previous contents readable.)

_____ Validate the content of each file using "String search" identification software i.e., BUSTER and perform a physical review of each file/line identified during the string search:

_____ Conduct a baseline audit of each file to ensure configuration control, i.e., CHECKSUM, if available:

_____ Conduct the file transfer using appropriate utility software, i.e., SECURE COPY from the source environment to the target environment.

_____ Virus scan, ensure disk is write protected:

_____ Overwrite all unused space on the target environment using appropriate utility software i.e., FLUSH:

_____ Conduct a static review of random files (at least 20 blocks of data) on the target device:

_____ Re-certify the contents of the target device by executing both string-search (BUSTER) and audit (CHECKSUM) utilities:

_____ Label target device (media) with the correct classification/handling requirements.

_____ Return this completed form to the command ISSM for retention.

I certify that all procedures outlined above were completed and this data transfer was accomplished without incident.

Signature

Date

MAY 10 2004

APPENDIX E

PROCUREMENT OF FORMS

The forms, with stock numbers, listed below are used in conjunction with the Information and Personnel Security Program.

These forms are procured through the local SERVMART or through the Naval Forms and Publications Supply System.

DD Form 254	Contract Security Classification 0102-LF-011-5800
DD Form 844	Request For Duplication 0102-LF-000-8440
OPNAV 5216/10	Correspondence/Material Control 0107-LF-052-1650
OPNAV 5510/21	Security Container Record Form 0107-LF-783-5100
OPNAV 5511/12	Classified Material Destruction Report 0107-LF-055-1160
OPNAV 5521/27	Visit Request 0107-LF-055-2235
Standard Form 700	Security Container Information 7540-01-214-5372
Standard Form 701	Activity Security Check List 7540-01-213-7899
Standard Form 702	Security Container Check Sheet 7540-01-213-7900
Standard Form 703	Top Secret Cover Sheet 7540-01-213-7901
Standard Form 704	Secret Cover Sheet 7540-01-213-7902
Standard Form 705	Confidential Cover Sheet 7540-01-213-7903
Standard Form 706	Top Secret Label 7540-01-207-5536
Standard Form 707	Secret Label 7540-01-207-5537

NETPDTCINST 5510.1B

MAY 10 2004

Standard Form 708	Confidential Label 7540-01-207-5538
Standard Form 709	Unclassified Label 7540-01-207-5539
Standard Form 710	Classified Label 7540-01-207-5540
Standard Form 711	Data Descriptor Label 7540-01-207-5541
CNET-GEN-5521/1	Classified Material Access Certification 0197-LL-NF3-1493

MAY 1 0 2004

APPENDIX F

EXTRACTS FROM THE ESPIONAGE LAWS AND FEDERAL STATUTES**UNITED STATES CODE, TITLE 18, SECTION 793 - GATHERING,
TRANSMITTING OR LOSING DEFENSE INFORMATION:**

a. Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work or defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored or are the subject of research or development, under any contract or agreement with the United States or any department of agency thereof, or with any person on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

b. Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, made, or obtain any sketch, photograph, photographic negative, blueprint, plan, map model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

c. Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance or note of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made or disposed of by any person contrary to the provisions of this chapter; or

MAY 10 2004

d. Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense, when information the possessor has reason to believe could be used to the injury of the United States or the advantage of any could be used to the injury of the United States or the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

e. Whoever, having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the office or employee of the United States entitled to receive it; or

f. Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map model, instrument, appliance, note or information relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer - Shall be fined not more than \$10,000 or imprisoned not more than ten (10) years, or both.

MAY 10 2004

g. If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. June 25, 1948, c. 645, Section 1, 62 Stat. 736, amended Sept. 23, 1958, c. 1024, Section 18, 64 Stat.

UNITED STATES CODE TITLE 18, SECTION 794 - GATHERING OR DELIVERING DEFENSE INFORMATION TO AID FOREIGN GOVERNMENT:

a. Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

b. Whoever, in time of war, with intent that same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

c. If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. As amended Sept. 3, 1954, c. 1261, Title II, Section 201, 68 Stat. 1219.

UNITED STATES CODE, TITLE 18, SECTION 795 - PHOTOGRAPHING AND SKETCHING DEFENSE INSTALLATIONS:

MAY 1 0 2004

a. Whenever, in the interest of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative, thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station or naval vessels, military or naval command concerned, or higher authority, and promptly submitting the product obtained to such command officer, or higher authority for censorship or such other action as he may deem necessary.

b. Whoever, violates this section shall be fined not more than \$1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 737).

UNITED STATES CODE, TITLE 18, SECTION 796 - USE OF AIRCRAFT FOR PHOTOGRAPHING DEFENSE INSTALLATIONS:

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment in violation of Section 795 of this title, shall be fined not more than \$1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62, Stat. 738).

UNITED STATES CODE, TITLE 18, SECTION 797 - PUBLICATION AND SALE OF PHOTOGRAPHS OF DEFENSE INSTALLATIONS:

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under Section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fine not more than \$1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 738).

UNITED STATES CODE, TITLE 18, SECTION 798 - DISCLOSURE OF CLASSIFIED INFORMATION:

~~MAY~~ 10 2004

a. Whoever, knowingly, and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information - (1) concerning the nature, preparation or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair or any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for crypto-graphic or communication intelligence purpose; or (3) concerning the communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes - Shall be fined not more than \$10,000 or imprisoned not more than ten (10) years or both. (Added Oct. 31, 1951, ch. 655, Section 24(a), 65 Stat. 719).

UNITED STATES CODE, TITLE 50, SECTION 797

a. Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics, or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress there to or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage, or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed \$5,000 or to imprisonment for not more than one year, or both.

b. Every such regulation or order shall be posted in conspicuous and appropriate places. (Sept. 23, 1950. ch. 1024, Title I, Section 21, 64 Stat. 1005.)

UNITED STATES CODE, TITLE 18, SECTION 1001

~~MAY~~ 10 2004

Whoever, in any matter within the jurisdiction of any department or agency of the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme or device, a material fact or makes any false, fictitious or fraudulent statements or representations or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined not more than \$10,000 or imprisoned not more than five (5) years, or both.

UNITED STATES CODE, TITLE 50, SECTIONS 783 (B) AND (D)

b. It shall be unlawful for any officer or employee of the United States or any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of Section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President or by the head of the department, agency or corporation by which this officer or employee is employed, to make such disclosure of such information.

d. Any person who violates any provision of this Section shall, upon conviction thereof, be punished by a fine of not more than \$10,000, or imprisonment for not more than ten (10) years, or by both such fine and such imprisonment, and shall moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

MAY 1 0 2004

UNIFORM CODE OF MILITARY JUSTICE**Article 106a ESPIONAGE**

(a) (1) Any person subject to this chapter who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any entity described in paragraph (2), either directly or indirectly, any thing described in paragraph (3) shall be punished as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court-martial may direct.

(2) An entity referred to in paragraph (1) is--

- (A) a foreign government;
- (B) a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States; or
- (C) a representative, officer, agent, employee, subject or citizen of such a government, faction, party, or force.

(3) A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

(b) (1) No person may be sentenced by court-martial to suffer death for an offense under this section (article) unless--

- (A) the members of the court-martial unanimously find at least one of the aggravating factors set out in subsection (c); and
- (B) the members unanimously determine that any extenuating or mitigating circumstances are substantially outweighed by any aggravating circumstances, including the aggravating factors set out under subsection (c).

(2) Findings under this subsection may be based on--

- (A) evidence introduced on the issue of guilt or innocence;
 - (B) evidence introduced during the sentencing proceeding;
- or
- (C) all such evidence.

MAY 10 2004

(3) The accused shall be given broad latitude to present matters in extenuation and mitigation.

(c) A sentence of death may be adjudged by a court-martial for an offense under this section (article) only if the members unanimously find, beyond a reasonable doubt, one of more of the following aggravating factors:

(1) The accused has been convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute.

(2) In the commission of the offense, the accused knowingly created a grave risk of substantial damage to the national security.

(3) In the commission of the offense, the accused knowingly created a grave risk of death to another person.

(4) Any other factor that may be prescribed by the President by regulations under section 836 of this title (Article 36).