

20 JUL 1987

NAS OCEANA INSTRUCTIONS 5510.2

Subj: NAVAL AIR STATION OCEANA SECURITY PLAN FOR INFORMATION AND PERSONNEL SECURITY

Ref: (a) OPNAVINST 5510.1G

1. Purpose. To provide personnel with regulations and guidance for classifying and safeguarding classified material and to establish procedures for personnel security.
2. Scope. This instruction is the basic directive for the implementation of the Department of the Navy Security program at this command.
3. Objective. To implement applicable requirements of reference (a) and establish procedures to assist the Command Security Manager in protecting, handling, controlling and accounting for classified material, and to ensure maximum uniformity and effectiveness in the application of the security regulations contained in reference (a) by Naval Air Station Oceana.
4. Discussion. A viable information security program must receive command attention and direction. It must function at all echelons in the chain of command and must be carried out by personnel who are properly trained.
 - a. Reference (a) establishes overall policy regarding information and personnel security. In view of recent procedures to tighten security, this instruction provides additional working guidance necessary for the overall handling of security.
 - b. The provisions of this instruction apply throughout Naval Air Station Oceana.
 - c. Departments are invited to submit recommendations for changes and/or revisions to this instruction.
5. Responsibility
 - a. All individuals in the naval service and civilians employed by the Department of the Navy are directly responsible for the security of classified information.
 - b. The Command Security Manager is the Commanding Officer's advisor and direct representative and is responsible for implementing this instruction.
 - c. Department heads and special assistants are responsible for compliance with reference (a) and this instruction. They will ensure that all personnel are informed of their responsibilities to safeguard classified information or equipment entrusted to them. They will ensure that only the absolute minimum number of personnel with a need-to-know are authorized clearance and access to classified material.
5. Action
 - a. The Security Manager and those individuals appointed in support of the security program will be thoroughly familiar with reference (a) and this instruction. The Security Manager will ensure that individuals within the command are familiar with reference (a), this instruction and local security requirements.
 - b. Department heads and special assistants shall ensure that security procedures outlined in reference (a) are adhered to and all individuals are familiar with the requirements defined in this instruction.


J. E. ALLEN

Distribution:
NASOCEANA INST 5216.1G
List 1, 2, 3, 4 (1 copy)

TABLE OF CONTENTS

	<u>Page</u>
Chapter I	
Program Management	
1-1 Command Management	1
1-2 Command Security Manager	1
1-3 Assistant Command Security Managers	1
1-4 Top Secret Control Officer	2
1-5 ADP Security Officer	2
1-6 Communications Material Systems (CMS) Custodian	3
1-7 Naval Warfare Publications Library (NWPL) Custodian	3
1-8 Department Heads/Special Assistants	4
1-9 Civilian Personnel Officer	4
1-10 Department/Office Security Coordinators	4
Chapter II	
Security Education	
2-1 Purpose of Security Education Program	1
2-2 Objectives	1
2-3 Scope and Content	1
2-4 Refresher Training	1
2-5 Indoctrination Briefing	2
2-6 Operational Security (OPSEC) Briefings	2
2-7 Counter-Intelligence/Espionage Briefings	2
2-8 Special Briefings	2
2-9 Debriefings	3
FIGURE 2-A NAS Oceana Form 5510/1 (New 4-87); Security Briefing Statement	
FIGURE 2-B Foreign Travel Briefing	
Chapter III	
Personnel Security	
3-1 Basic Regulations	1
3-2 Granting Security Clearances	2
3-3 Access Authorization	4
3-4 Emergency Access	5
3-5 Process for Requesting Clearance and/or Access Authorization	5
3-6 Certificate of Clearance	6
3-7 Classification Information Non-disclosure Agreement (SF-189)	6
3-8 Termination of Personnel Security Clearance/Access	6
3-9 Security Termination Statements	6
3-10 Administrative Withdrawal	7
FIGURE 3-A Request for Emergency Appointment To A Critical-Sensitive Position	
FIGURE 3-B Request for Emergency Appointment To A Noncritical-Sensitive Position	
FIGURE 3-C Request for Emergency Access Pending Results of Investigation	
FIGURE 3-D Request for Civilian Security Clearance	
FIGURE 3-E Classified Information Non-disclosure Agreement (SF-189)	
FIGURE 3-F Security Terminating Statements OPNAV 5511/14	

	<u>Page</u>
Chapter IV Security Violations	
4-1 Definition and Policy	1
4-2 Reporting Violations	1
4-3 Processing Violations	1
4-4 Preliminary Inquiry/Investigation/JAG Manual Investigation	1
4-5 Security Discrepancies	2
4-6 Inspection of Spaces	2
FIGURE 4-A Security Violation Report NAS Oceana FORM 5510/4	
FIGURE 4-B JAG Manual Investigation Checklist	
Chapter V Accountability and Control	
5-1 General	1
5-2 Document Control Points	1
5-3 Correspondence/Material Control Form (MCF) OPNAV Form 5216/10	2
5-4 Control and Routing	3
5-5 Inventories of Classified Material	5
5-6 Reproduction	5
FIGURE 5-A Correspondence/Material Control (4 PT) OPNAV 5216/10	
FIGURE 5-B Inventory Stamp	
FIGURE 5-C Inventory of Classified Material NAS Oceana Form 5511	
FIGURE 5-D Classified Container Inventory Sheet NAS Oceana Form 5511/1	
FIGURE 5-E Warning - Do Not Use For Classified	
FIGURE 5-F Warning - Use Only For Unclassified and Confidential Only	
Chapter VI Storage	
6-1 Responsibility	1
6-2 Stowage Containers	1
6-3 Location and Maintenance of Security Containers	1
6-4 Combinations	1
6-5 Combination Changes	2
6-6 Safe or Cabinet Security Record	2
6-7 Equipment Records Management	2
6-8 Equipment Types and Specifications	3
6-9 Stowage of Classified Equipment/Parts	3
6-10 Custodians/Security Coordinators Stowage Responsibilities	3
6-11 Stowage Prohibitions	4
6-12 Non-Classified Stowage	4
FIGURE 6-A Standard Form 700	
FIGURE 6-B Classified Container Information OPNAV 5511/30	
FIGURE 6-C Privacy Act Statement (GSA Standard Form 700 or OPNAV Form 5511/30)	
FIGURE 6-D Security Container Check Sheet Standard Form 702	
FIGURE 6-E Security Container Records Form (OPNAV 5510/21)	
FIGURE 6-F Non-Classified Stowage Tag NAS Oceana Form 5511/3	

20 JUL 1987

	<u>Page</u>
Chapter VII Safeguarding	
7-1 Custodial Responsibilities	1
7-2 Care During Normal Working Hours	1
7-3 Care and Stowage After Working Hours	2
7-4 Securing for the Day Procedures	2
7-5 Care During Emergencies	3
7-6 Classified Material Found Unattended After Normal Working Hours	3
7-7 Telephones	3
FIGURE 7-A Activity Security Checklist	
Chapter VIII Transmission	
8-1 Basic Policy	1
8-2 Guard Mail	1
8-3 Regular Mail System	1
8-4 Preparation of Envelopes or Containers	1
8-5 Classified Material Received in A Damaged Condition/Improperly Received	2
8-6 Receipt System	2
8-7 Transmission by Other Than Regular Mail	3
8-8 Courier Authorization Aboard NAS Oceana	3
8-9 Courier Authorization Off-Base NAS Oceana	3
8-10 Hand Carrying Classified Documents/Packages Aboard Commercial Aircraft	3
FIGURE 8-A Classified Material Courier Card NAS Oceana Form 5510/3	
FIGURE 8-B Courier Authorization Log	
FIGURE 8-C Designation As NAS Oceana Courier (Sample Letter)	
FIGURE 8-D Authorization to Carry Classified Material on Commercial Aircraft (Sample Letter)	
Chapter IX Destruction	
9-1 Policy	1
9-2 Method of Destruction	1
9-3 Responsibilities and Destruction Records	1
9-4 Burn Bags	2
9-5 Destruction Equipment	3
9-6 Emergency Destruction	3
Figure 9-A Classified Material Destruction Report OPNAV 5511/12	

Chapter X	Classification/Marking	Page
	10-1 Policy	1
	10-2 Classification Designations	1
	10-3 For Official Use Only	1
	10-4 Original/Derivative Classification	1
	10-5 Downgrading and Declassification	2
	10-6 Tempest	2
	10-7 Classification Markings	2
	10-8 Use of Cover Sheets	2
	10-9 Marking Components	3
	10-10 File or Folder Marking	3
	10-11 Portion and Paragraph Marking	3
	10-12 Warning Notices	3
	10-13 Electrically Transmitted Messages	3
	10-14 Marking of Card Decks	3
	10-15 Automatic Data Processing (ADP) Tapes and Word Processing Storage Media	3
	10-16 Conclusion	3
	FIGURE 10-A Marking Guide for Publications and Correspondence	
	FIGURE 10-B Security Classification Guides	
	FIGURE 10-C Schematic for Paragraph Marking	
	FIGURE 10-D Classified Message (Sample)	
Chapter XI	Control of Visitors	
	11-1 Incoming Visits	1
	11-2 Outgoing Visits	1
	11-3 Visits to Contractor Facilities	2
	11-4 Visits by Representatives of General Accounting Office	2
	11-5 Visits by Contractors	2
	11-6 Expiration of Visit Requests	2
	11-7 Visit Reports	2
	11-8 Meetings	2
	FIGURE 11-A Visit Request Message (Sample)	
Chapter XII	Emergency Plan for the Protection of Classified Material	
	12-1 General	1
	12-2 Implementation	1
	12-3 Procedures	1

CHAPTER I

PROGRAM MANAGEMENT RESPONSIBILITIES

1-1 Command Management. The Commanding Officer is directly responsible for safeguarding all classified information at NAS Oceana. He has delegated the overall coordination of the Command Security Program to the Administrative Officer/Command Security Manager. Responsibilities for various specific areas are further delegated and assigned as follows.

1-2 Command Security Manager. The Command Security Manager is the principal advisor on information and personnel security in the command and is responsible for the management of the program. He/she will report to the Commanding Officer on matters of security, but is responsible to the Executive Officer for administration of the Information and Personnel Security Program. The Command Security Manager will be appointed in writing and will:

1. Serve as the Commanding Officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security.
2. Develop written command information and personnel security procedures, including an emergency plan.
3. Formulate and coordinate the security education program for the command.
4. Ensure that threats to security, compromises and other security violations are reported, recorded and investigated.
5. Administer the command's program for classification and downgrading of classified information.
6. Coordinate the preparation of classification guides in the command, if required.
7. Maintain liaison with the command's public affairs officer to ensure that proposed press releases which could contain classified information are referred for security review.
8. Ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.
9. Formulate and coordinate physical security measures for protection of classified material.
10. Ensure security control of classified visits to and from the command.
11. Ensure protection of classified information during unclassified visits to the command.
12. Ensure that all personnel who handle classified information or are assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.
13. Ensure that access to classified information is limited to those with the need to know.
14. Ensure that personnel security investigations, clearances and access' are recorded.
15. Coordinate the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

1-3 Assistant Command Security Managers. The Assistant Command Security Managers will assist the Command Security Manager in all actions required to carry out the program as described in this instruction and will be appointed in writing. Each of the Assistant Command Security Managers will be tasked with carrying out responsibilities that are directly in support of the Security Program. The Assistant Security Manager for Information and Personnel Security will be responsible for:

1. The receipt, custody, storage, accountability and distribution of secret and confidential classified material within the command and its transmission outside the command, except the material distributed by the Communications Security Material System (CMS).

2. Ensuring that physical inventories of secret and confidential classified material are conducted at least twice annually.

3. Act as the Personnel Security Officer and, as such, ensure that clearance and access paperwork for military personnel is processed in accordance with reference (a) and this instruction.

The Assistant Security Manager for Training will be responsible for:

1. Training provided during the base indoctrination brief.

2. Training aides, such as films, being available for general military training.

3. Ensuring that the annual security brief is conducted and that all personnel, civilian and military, are offered an opportunity to participate.

4. Ensuring that posters and POD notes are utilized to publicize security requirements and that the education program is providing information throughout the air station.

5. Acting as the Command Operations Security Officer, will be familiar with OPNAVINST 3070.1 and CINCLANTFLTINST 3070.1 and responsible for training command personnel in the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling and protecting indicators associated with planning and conducting military operations and other activities.

1-4 The Top Secret Control Officer (TSCO) is responsible under the Command Security Manager, for the receipt, custody, accountability and distribution of Top Secret information within the command and its transmission outside the command, except the material distributed by the Communications Security Material System (CMS). The Top Secret Control Officer will be appointed in writing and will:

1. Inform the Commanding Officer, Executive Officer, Security Manager and authorized personnel who have the need to know of top secret material in his/her custody.

2. Ensure that top secret is not used by personnel working alone.

3. Personally receive, distribute, stow and account for all courier mail and top secret information not distributed by the Communication Security Material System.

4. Transmit top secret information within the command by direct personal contact.

5. Maintain a continuous chain of receipts for top secret material and a perpetual top secret inventory of material received, transferred or maintained by NAS Oceana.

6. Maintain a disclosure log for each item of top secret information.

7. Ensure that physical inventories of top secret material are conducted at least once annually and upon relief of TSCO or the Commanding Officer.

8. Maintain a current roster of personnel within the command who are authorized access to top secret information.

1-5. ADP Security Officer. The ADP Security Officer (ADPSO) will be appointed in writing and is the collateral duty of the Data Processing Department Head. The control and safeguard of classified ADP storage media and output is required in a manner equivalent to that protecting classified documents of a similar classification. The ADPSO will comply with OPNAVINST 5239.1 and will:

1. Coordinate with the Command Security Manager on matters concerning ADP security in accordance with the security organizational structure established by the Commanding Officer.

2. Ensure that an activity ADP Security Plan (AADPSP) is developed and maintained.

3. Ensure that an ADP System Security Officer (ADPSSO) is appointed in writing where applicable. When ADPSSO's are appointed, the ADPSSO will advise and assist the ADPSSO's and review their plans and procedures for completeness and adherence to policy.
4. Ensure that a Terminal Area Security Officer (TASO) is appointed where applicable for each remote terminal or cluster of interface devices.
5. Ensure that an Office Information Systems Security Officer (OISSO) is assigned to each Office Information System (OIS).
6. Ensure that an effective activity Risk Management Program is implemented.
7. Ensure that requests for accreditation of ADP activities and networks are completed in accordance with the procedures prescribed in OPNAV INST 5239.1 (series).
8. Ensure that all ADP security incidents or violations are investigated, documented and reported.
9. Ensure that security requirements are included in life cycle management documentation as prescribed in SECNAV Instructions 5000.1 or 5231.1 (series), as appropriate.
10. Ensure that all procurement documents or specifications approved within the activity comply with appropriate ADP security requirements.
11. Ensure the development and testing of all contingency plans.
12. Ensure that Naval Audit Service (NAVAUDSVC) is advised of the development of an ADP system, as applicable.
13. Ensure that accreditation support documentation is developed and maintained.
14. Assist the ADP security staff in implementing their respective ADP security responsibilities.
15. Ensure that applicable personnel security procedures are established for all ADP activities and networks.
16. Ensure that Security Test and Evaluation's (ST&E's) are conducted.
17. Develop a Commanding Officer's Risk Assessment Team Charter and Plan of Action and Milestones (POA&M).
18. Maintain an inventory of all command ADP and OIS equipment.
19. Monitor system activity to ensure compliance with security directives and procedures, including the types and sensitivity of the data handled by the ADP/OIS system.
20. Control, issue and maintain passwords for terminal users.
21. Ensure terminal passwords are replaced at least every six months on a non-scheduled basis.
22. Ensure NAS Oceana compliance with Department of the Navy (DON) Automatic Data Processing Program Reporting System (ADPPRS).

1-6 Communications Material Systems (CMS) Custodian. The CMS custodian is responsible for the Communications Material System for NAS Oceana. He/she will carry out duties in accordance with the Communications Material Systems Manual (CMS-4) and will report to the Commanding Officer via the Executive Officer and Command Security Manager.

1-7 Naval Warfare Publications Library (NWPL) Custodian. The NWPL custodian is responsible for the Naval Warfare Publications Library at NAS Oceana and will carry out his/her duties in accordance with NWP O, Chapter II. Naval Warfare publications, classified or unclassified, have their own system for administration.

20 JUL 1987.

1-8 Department Heads/Special Assistants. Department heads/special assistants are responsible for ensuring that all classified information received, retained or imparted within their department is afforded the safeguards outlined in reference (a). This is a continuing requirement which must be the subject of personal attention on a periodic basis. Positive and repetitive action must be taken to preclude a complacent and apathetic attitude toward the security of classified information by department personnel. Department heads/special assistants are responsible for the promulgation of additional directives and/or guidance (with copies to the Command Security Manager) that may be required to prevent unauthorized disclosure of classified information under their control.

1. Department heads/special assistants will ensure that all persons who are to handle classified information are immediately instructed in their responsibilities and cleared pursuant with reference (a).

2. Department heads/special assistants will designate in writing an officer, senior enlisted or civilian to serve as the Department Security Coordinator. A signed copy of this designation will be forwarded to the Command Security Manager.

1-9 Civilian Personnel Officer. The Civilian Personnel Officer is responsible for ensuring a member of his/her staff is assigned the responsibilities of administering the personnel security program for all civilians assigned to this air station. This involves the proper administration and processing of civilian security clearance requests in accordance with reference (a) and NCPCINST 5521.1. It also involves the proper accounting, identification and control of all civilian positions requiring clearances and the ability to report the same to the Command Security Manager.

1-10 Department/Office Security Coordinators. The department/office security coordinators will be designated in writing by the appropriate department head and will report to the Security Manager concerning attainment of all requirements within this instruction. The department/office security coordinators are required to institute all requirements of this instruction within their department. They will identify specific security requirements for their organizational element and ensure proper and adequate procedures are followed at all times. The department/office security coordinator will:

1. Be thoroughly familiar with OPNAVINST 5510.1 (series), Information and Personnel Security - Program Regulation.

2. Serve as the department head/special assistant advisor and direct representative to the Command Security Manager.

3. Formulate and coordinate the security education program within their respective department.

4. Develop an emergency destruction bill to be incorporated into the station's emergency plan where required.

5. Ensure that threats to security, compromises and other security violations are reported immediately to the Command Security Manager.

6. Ensure all department work is classified, declassified and downgraded properly or referred to the Assistant Command Security Manager (Admin Support Services Supervisor).

7. Ensure compliance with accounting and control requirements for classified material, including:

- a. Receipt
- b. Distribution
- c. Inventory
- d. Reproduction
- e. Disposition
- f. Destruction
- g. Storage

8. Formulate and coordinate physical security measures for protection of classified material/equipment.
9. Ensure security control of classified visits to and from the command and that all requests for classified visits are submitted via the Command Security Manager.
10. Ensure the protection of classified information during unclassified visits to the command.
11. Ensure compliance with the industrial security program for classified contact with DOD contractors.
12. Ensure that all personnel who are to handle classified information/equipment are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.
13. Ensure that access to classified information/material/equipment is LIMITED to those with the need to know.
14. Ensure department/office personnel have clearance and access recorded.
15. Continually evaluate access eligibility.

CHAPTER II
SECURITY EDUCATION

2-1 Purpose. Basic to the Security Education Program is the appreciation for the need to protect classified and sensitive information. The information security program is necessary because there is information essential to national security or the rights of individuals that must be protected. In the case of classified information it must be protected from foreign intelligence services, whereas information concerning an individual must be protected against errors, omissions and general disclosure under the Privacy Act of 1974.

2-2 Objectives

1. The objectives of the security education program are to advise personnel of:
 - a. The need for protecting classified and privacy information.
 - b. The adverse effects to the national security resulting from unauthorized disclosure.
 - c. The personal responsibilities for protecting the information in their possession.
 - d. Specific security procedures.
 - e. Procedures for challenging classification decisions.
 - f. Techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility to report such attempts.
 - g. The hazards involved and the strict prohibition against discussing classified information over the telephone or in any such manner as to be intercepted by unauthorized persons.
 - h. Disciplinary actions that may result from violation of security regulations.
 - i. Indoctrinate personnel on the proper procedures for the handling, accountability and storage of command classified material.
 - j. Indoctrinate personnel on the proper procedures for reporting and investigating command security violations.

2-3 Scope and Content. The Security education program is to be designed to result in the positive reinforcement of sound security practices. Certain types of security briefings are required by the Security Manual (OPNAVINST 5510.1). The Command Security Manager or his/her representative will conduct these briefings. The minimum requirements are:

1. Refresher Training - given annually to all employees through general military training or civilian professional training.
2. Indoctrination Briefing - given to all personnel as soon after reporting aboard as possible.
3. OPSEC Briefing - presented annually.
4. Counter Intelligence/Espionage Briefing - presented annually.
5. Debriefings - given to all individuals upon termination of service, employment or revocation of clearance.

2-4 Refresher Training. It is important that all employees, not only those having access to classified information, have a basic understanding of what is meant by "classified information" and how it is protected. The General Military Training directive, OPNAVINST 1500.22, describes the objectives for Navy members. As a minimum, the command program is to include an annual briefing on security. The purpose of having this requirement, in addition to other security briefing requirements, is to ensure that all employees know there is information to be protected and to give them all an idea of how it is to be protected so they will recognize breaches of security. All personnel should know:

20 JUL 1987

1. Certain information, essential to national security, requires protection from disclosure to unauthorized persons.
2. Information subject to the Privacy Act of 1974 is to be protected.
3. Classified material is marked to show the level of classification.
4. Only those who have been granted security clearances may have access to classified information and then only on a need-to-know basis.
5. There are basic methods for storing and disposing of classified material.
6. That any breach of security must be reported at once to the Command Security Manager.
7. That any contact in any form with any citizen of a communist controlled country must be reported.
8. Who the Command Security Manager is by name.
9. Changes in policy or procedure concerning security.

2-5 Indoctrination Briefing

1. Newly reporting personnel shall be indoctrinated during check-in procedures in the importance of maintaining the highest standards of security, the basic policies and procedures employed for this purpose and their responsibilities as part of this security program. Security training for these individuals shall include, as a minimum, the following: A short oral and written security indoctrination briefing in the general requirements for access to classified material, office working-hours security, after-hours security procedures and OPSEC security. This briefing will be furnished during the base indoctrination program and will be presented by the Assistant Security Manager for Training.

2. Department/Office Security Coordinators shall:

a. Brief all newly reporting personnel in local security practices within three working days of their assignment to that department. After signing the department brief section of Security Briefing Statement (NAS OCEANA Form 5510/1) Figure 2-A, the form will be retained by the Department/Office Security Coordinator.

b. Provide those individuals who will specifically handle classified material or equipment with copies of local security instructions and shall require them to become familiar with these provisions.

c. Conduct a continuing program of security training. Department security training programs shall encompass all phases of handling, stowage and safeguarding of classified information and shall be tailored to the peculiarities of department office spaces, equipment, mission and tasks. The Command Security Manager will assist, as required, in enhancing their security training program. Reports of such training will be forwarded to the Command Security Manager for command security training reports.

2-6 OPSEC Briefings

1. All permanently assigned personnel, military and civilian, will receive an OPSEC briefing annually and OPSEC training at indoctrination. The Assistant Command Security Manager for training is the OPSEC Officer.

2. All department training will include related OPSEC training.

2-7 Counter-Intelligence/Espionage Briefing. This briefing will be given annually to all personnel. The Assistant Security Manager for Training will schedule with NIS to have an agent conduct the briefing.

2-8 Special Briefings. Special briefings will be coordinated through the Command Security Manager on an as required basis, such as foreign travel briefings, Figure 2-B.

2-9 Debriefings

1. When individuals are separated from the command by end of service or termination of employment, they are to be given a security debriefing by the Department/Office Security Coordinator. The debriefing session is to make it clear to the individuals that they are certifying that:

a. They do not have classified/sensitive material in their possession.

b. They will not divulge classified/sensitive information to an unauthorized person and that there are penalties for such disclosures.

c. They have read and understood Appendix F of the Information Security Program Regulation (OPNAVINST 5510.1 (series)).

d. Once they execute the Security Termination Statement, they are liable to prosecution if the certification is false.

2. Any individual who refuses to sign the statement will be briefed, with emphasis on the fact that refusal to sign does not negate the individual's obligation to protect classified information from unauthorized disclosure. In such cases, the Security Termination Statement will be so annotated and a copy forwarded to the Command Security Manager who will forward to CNO (OP-0090).

3. Any individual who has had special access (NATO, SCI, etc.) must also be given a debrief by the Command Security Manager or designated individual.

20 JUL 1987

FOREIGN TRAVEL BRIEFING

1. In view of the recent terrorist actions, the increase in harassment and violent attacks against innocent travelers is cause for grave concern. The unstable international climate dictates heightened awareness and safety/security conscientiousness on the part of all U.S. citizens, particularly those traveling in Europe and the Middle East. There is clear evidence that U.S. military personnel and DOD civilian employees continue to be prime targets for harassment and terrorist attacks.
2. The following guidance is provided to assist you while traveling overseas. These countermeasures should lower the symbolic profile and increase your chances of survival.
 - a. When military airlift cannot be used for mission essential travel to, from and through Middle East countries, and when intratheater travel must be performed via commercial aircraft to, from and through high risk areas, tourist passports shall be used unless prohibited by the foreign country to be visited.
 - b. Travel should be in civilian clothing except on military aircraft.
 - c. Distinctive military items should not be worn with civilian attire, e.g., black shoes, belts, dog tags or unit insignia on key chains, etc.
 - d. Nondescript civilian clothing should be worn. Do not wear apparel clearly of U.S. origin such as cowboy hats, belt buckles, etc.
 - e. Documents identifying affiliation with the U.S. Government should not be carried onto commercial aircraft, e.g., service club and business cards, checkbooks with rank and military address, distinctive military decals, Government driver's licenses, insurance papers, military jewelry, etc.
 - f. Compromising items like identification cards, travel orders and airline tickets bearing a base validation stamp should be carried in "checked" baggage or together in a readily assessable pocket or outside unzipped pouch of your carry-on luggage so that in the event of a hijacking, these items can be pushed into a seat, magazine or other hiding place. Window seats offer more protection and are harder to search.
 - g. Baggage identification should not identify military rank or insignia. Handcarried briefcases should have no military slogans or emblems on the outside and no official papers inside.

20 JUL 1987

- h. Obtain written authorization on travel orders to wear civilian clothing when traveling on military aircraft connecting with a commercial flight which will transit a terrorist threatened area.
- i. All references to military rank should be eliminated on documents used to arrange or coordinate travel, e.g., itineraries.
- j. Baggage I.D. should not indicate military rank, insignia or duty station.
- k. Out-of-Conus travelers requiring overnight lodging should use U.S. facilities such as BOQ/BEQs or other U.S. approved facilities.
- l. Avoid loitering in public sections of an airport. When possible, proceed expeditiously through security checkpoints to secure areas to await flight.
- m. Purchase tickets prior to arrival at the airport to minimize time spent in unsecured areas.
- n. Arrive at the airport early to preclude standing in line for check-in prior to movement to controlled areas.
- o. For maximum safety, personnel flying civilian airlines should wait for departing aircraft from within the controlled area. Minimize time spent in unsecured areas.
- p. Avoid crowded areas in airports as they provide lucrative targets for terrorists.
- q. All meetings held in foreign countries including military personnel should be conducted within the confines of military facilities.
- r. Use caution when visiting off-base overseas facilities known to be popular gathering places for U.S. military personnel.
- s. Do not discuss your military association with anyone.
- t. Devise a plausible cover story. The cover story should be simple and include as much accurate and verifiable information as possible. Stick to your story.
- u. Be aware that all hijackers may not reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by the other hijackers.

20 JUL 1987

CHAPTER III

PERSONNEL SECURITY

3-1 Basic Regulations. Chapter 21 of OPNAVINST 5510.1 (series) provides detailed information on types of personnel security investigations (PSI), the satisfactory completion of which shall form the basis for and precede the granting of access to classified defense information. PSI is used to describe the inquiry into an individual's activities and is conducted to determine that the individual's acceptance for military service or civilian employment is clearly consistent with the interests of national security or to establish eligibility for security clearances or assignment to other sensitive duties. Types of investigations are as follows:

1. National Agency Check (NAC) and Entrance NAC (ENTNAC) - a check of the files of federal agencies conducted by Defense Investigative Service (DIS).
2. National Agency Check and Inquiry (NACI) - an Office of Civilian Personnel investigation, conducted on civilians only which consists of a NAC - check of the files of federal agencies - plus written inquiries to law enforcement agencies, former employers, supervisors, references and school officials.
3. Background Investigation (BI) - conducted by DIS, consisting of a NAC check and field investigation by interview and written inquiry to develop information about the individual's loyalty, character, emotional stability and reliability.
4. Special Background Investigation (SBI) - conducted by DIS, includes same type investigation as for BI, but is an extended coverage of the individual's background providing greater depth of knowledge.
5. Post-Adjudication Investigation - conducted by DIS to develop facts relating to a specific incident or item of information. Usually requested to resolve unfavorable information, except that which involves current criminal activity, sabotage or subversion.
6. DCII - conducted by the Naval Security and Investigative Command (NSIC), is a review of files including those of the Naval Military Personnel Command (NMPC).
7. Investigative requirements for military personnel for the Naval Service are contained in instructions issued by NMPC.
 - a. Top Secret - for a final clearance, a background investigation is required. An interim clearance may be granted with a NAC or ENTNAC if the BI investigation has been requested.
 - b. Secret - a final clearance may be granted based on a NAC or ENTNAC. An interim clearance may be granted on the basis of a name check by NSIC and an ENTNAC or NAC requested.
 - c. Confidential - final clearance requires a NAC or ENTNAC.
 - d. NATO - a final U.S. clearance at the equivalent level.
8. Investigative requirements for the employment of civilian personnel in the Department of the Navy are established by Naval Security and Investigative Command, along with the standards, criteria and administrative procedures governing the disposition of security cases involving civilian employees and applicants.
 - a. Top Secret or Critical Sensitive Position - a BI is required for a final clearance. An interim clearance and emergency appointment may be granted based on:
 - (1) a satisfactory NACI, ENTNAC or NAC if BI has been requested,
 - (2) a favorable check of locally available records has been made, and
 - (3) an emergency appointment has been justified in writing by the appropriate department head (Figure 3-A through Figure 3-C).

20 JUL 1987

b. Secret, Confidential, or Noncritical-Sensitive Position - a NACI is required for a final clearance. An interim clearance and emergency appointment may be granted based upon:

- (1) a favorable check of locally available records,
- (2) a satisfactory check of the Defense Central Index of Investigations by NSIC,
- (3) the initiation of a NACI, and
- (4) an emergency appointment has been justified in writing by the appropriate department head.

9. Modification of Requirements. Minimum investigative requirements which must be met prior to the granting of a security clearance are specified in OPNAVINST 5510.1 (series). These requirements shall not be reduced or modified in any way in the granting of security clearances to NAS Oceana personnel, except under emergency situations as provided in paragraph 3-4 of this instruction.

3-2 Granting Security Clearances

1. The Commanding Officer assumes the authority and is charged with the responsibility for granting or denying security clearances and access to classified information at NAS Oceana. The Command Security Manager is hereby delegated the authority to sign certificates of personnel clearance "By direction" of the Commanding Officer.

a. All military personnel assigned to NAS Oceana will check in and out with the Assistant Security Manager for Information and Personnel Security (Admin Support Services Office).

b. All civilian personnel will check in and out with the employment division of the Civilian Personnel Department.

2. The Command Security Manager is responsible for the proper handling of requests for security investigations, evaluation of investigative data, the issuance of personnel clearances and the granting of access to classified material.

3. Department heads are responsible for determining the clearance categories/levels of positions/billetts of their departments. Assistance may be obtained from the Civilian Personnel Department or the Command Security Manager.

a. When an individual reports aboard, a determination will be made as to whether that person needs access to do his job and the level of access necessary. That decision is not a permanent judgement. Access granted will reflect current need. As the individual's duties may change, requiring a greater or lesser degree of access, the access granted will be adjusted as necessary by the Department Security Coordinator. As granting access is a command responsibility, access will be terminated when the individual transfers from the command. When access must be adjusted, the Department Security Coordinator will forward a memo to the Assistant Security Manager (Admin Support Services Supervisor) for military personnel and to the Employee Division of CPD for civilian personnel.

b. The following is a general guideline for determining civilian clearance requirements.

(1) Position Sensitivity. A sensitive position is any position the occupant of which could bring about, by virtue of the nature of their position, a material adverse effect on the national security.

(2) For investigative purposes, there are three general categories of civilian positions in the Department of the Navy: critical-sensitive, noncritical-sensitive and non-sensitive. The investigative requirements for appointment to and retention in the positions are defined below:

(a) Critical-Sensitive Position. Any position, the duties or responsibilities of which include:

- Access to top secret information.
- Involvement in the development or approval of plans, policies or programs that affect the overall operations of the Department of the Navy.
- Involvement in the development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.
- Involvement in the investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations or the making of personnel security determinations.
- Assignment to fiduciary, public contact or other duties demanding the highest degree of public trust.
- Assignment to duties requiring access to sensitive compartment information (SCI).
- Assignment to category I automated data program positions. (Note: This criterion will not be used to designate a position as critical-sensitive until further notice.)
- Assignment to any other position so designated by SECNAV or designees.

NCPCINST 5521.1 requires that civilians occupying a critical-sensitive position shall update their Statement of Personnel History Form (DD 398) every five years.

(b) Noncritical-Sensitive Position. Any position, the duties or responsibilities of which include:

- Access to secret or confidential information.
- Assignment to security police/provost marshal-type duties involving the enforcement of law, and security duties involving the protection and safeguarding of DON personnel and property.
- Assignment to duties involving education and orientation of DON personnel.
- Assignment to duties involving the design, operation and maintenance of intrusion detection systems deployed to safeguard DON personnel and property.
- Assignment to category II automated data program positions.
- Assignment to any other position so designated by the SECNAV or designees.

(c) Nonsensitive Position. Any position which does not involve duties and responsibilities categorized above.

c. The following is a general guideline for determining military requirements:

(1) Officers

(a) The security access for the Commanding Officer will be issued pursuant to Article 23-5 of OPNAVINST 5510.1 (series).

(b) The level of security access for the Executive Officer will be determined by the Commanding Officer.

20 JUL 1987

(c) The level of security access for other officers will be determined by the Commanding Officer, based upon a recommendation from the department head. The "need-to-know" precept applies in all cases, but as a minimum, all officers who stand CDO watches at this command will have at least a secret access.

(2) Enlisted

(a) Upon assignment of a newly reported enlisted person, the department head will determine the level of security access required in order for that individual to perform assigned duties. The "need-to-know" precept applies in all cases.

(b) All Chief Petty Officers (E7-E8) who stand OOD watches at this command will have at least a secret access.

(3) Foreign Exchange Personnel. CNO (OP-009) will issue a disclosure authorization for each foreign exchange individual by name. This authorization will be sent to the command to which the individual is assigned duty. The Command Security Manager will ensure that the department head to which the foreign exchange individual is assigned is notified of the level of disclosure authorized. It is the department head's responsibility to ensure that the foreign individual does not have access to any classified information other than that indicated in the disclosure authorization.

(4) Temporary Additional Duty. Military personnel reporting for temporary additional duty shall be cleared by their commanding officer prior to reporting and their clearance/access status reported to the Commanding Officer, NAS Oceana, in writing. Normally, such clearance/access will be accepted. Classified information may be disclosed after positive identification has been made and the department concerned has been convinced that a "need-to-know" exists.

4. Recruitment and Appointment to NAS Oceana Sensitive Positions

a. Civilian applicants will be informed by all interviewers that they will be subjected to security inquiry and that appropriate security clearance is a condition of employment. The individual will not be brought on board until the investigative requirements are met. Before hiring action will be initiated for any positions requiring a clearance, the department head will complete and forward Figure 3-D to CPD.

b. Department heads/special assistants will determine the position sensitivity when writing the position/job description. Assistance in making this determination can be provided by CPD or the Command Security Manager. All position/job descriptions for classification action will be routed through CPD for verification of sensitivity.

c. Approval by CPD of inter-command position changes will be required when an employee is reassigned from a noncritical sensitive position to a critical-sensitive position or from a nonsensitive position to a sensitive position.

d. The employee will remain assigned to nonsensitive or noncritical-sensitive duties until CPD notifies the cognizant department that a satisfactory clearance has been obtained.

e. Prior to transfer to NAS Oceana of any career civil service employee, CPD will review the status of the employee's security clearance which has been obtained from the prior command utilizing Standard Form 75. CPD will make available to the Commanding Officer (via the Command Security Manager) the file or any other material which may be required for adjudication of a security clearance in cases where the material seems to indicate the presence of possible derogatory or otherwise disqualifying information.

f. NAS Oceana will not hire any foreign nationals for sensitive positions since they cannot be granted a security clearance.

3-3 Access Authorization. It is important to recognize the distinction between holding a security clearance and having access authorization. The security clearance certifies that the facts made known of the individual's background and past activity establish his qualifications to receive classified information only if the "need-to-know" exists. The authorization for access indicates that, in addition to being eligible from a security standpoint, the person must have access to specific classified information in order to properly perform particular duties.

20 JUL 1987

1. The granting of access to classified material is a command function. The need is established by the specific duty being performed.
2. An access authorization does not entitle an individual access to all matter under the degree of classification. The individual is authorized only access for classified material for which they have a "need-to-know".
3. Access authorization shall not be issued to any individual just because they may meet the requirements for the respective classification.
4. A satisfactory completion of a NAC or a BI does not, in itself, constitute a clearance or an authorization for access. It merely establishes eligibility for a clearance and access authorization by the command.
5. When a person no longer needs access to a particular security classification category, the security manager should be notified and the security clearance shall be adjusted accordingly.
6. Continuous Evaluation for Access to Classified Information. Any person having knowledge or information that reflects adversely and indicates that an individual may no longer meet the criteria specified in paragraph 22-2 of OPNAVINST 5510.1 (series) shall immediately report the full particulars and circumstances to the Command Security Manager for evaluation and/or further investigation.

3-4 Emergency Access (Access Pending Clearance Requirements). The Commanding Officer may, only in cases of emergency, authorize access to classified information before the investigative requirements for final clearance have been completed. Prior to authorizing emergency access there has to be a written record of this authorization affirming that the procedures necessary for clearance have been initiated, that awaiting completion of the investigative requirements would cause a crucial delay in the training or assignment of the individual and that immediately available records have been reviewed and the individual is otherwise eligible for the access required. When the emergency access is for a civilian, the original of the report justifying emergency appointment will be retained by the Command Security Manager and an information copy will be forwarded to the Commander, Naval Security and Investigative Command (OP-09N). For military personnel, the emergency access letter will be retained by the Command Security Manager. Samples of these letters are shown in Figures 3-A, 3-B and 3-C.

NOTE: There is no provision for appointments to a critical sensitive position when the individual does not have any valid investigative basis.

3-5 Process for Requesting Clearance and/or Access Authorization

1. Department heads/special assistants requiring clearance and access authorization for military personnel within their department shall submit COMNAVAIRLANT Form 5521/1, Access to Classified Matter, in triplicate, to the Assistant Command Security Manager (Admin Support Services Supervisor).

NOTE: Keep in mind the number of clearances per department has already been established and restricted; clearances are extremely limited and controlled.

2. Upon receipt of the request, the Assistant Security Manager will determine the type of formal investigation, if any, required for the degree of access requested.

a. In the event further investigation is required, forms will be forwarded to the department head to be completed by the individual concerned and returned to the Assistant Security Manager for initiation of the investigation.

b. If no further formal investigation is required, the Assistant Security Manager will route the 5521 to medical, legal and the Personnel Support Detachment for records review. After processing is complete, the Security Manager will issue the appropriate clearance and access.

3. Department heads/special assistants requiring clearance and access authorization for civilian personnel within their department will ensure that the employment division at CPD has a complete and current listing of all positions requiring a clearance and access. The actual

20 JUL 1987

position description for which the employee is being hired must contain the proper clearance requirement. In the case of hiring, the department head must submit the 5521 prior to CPD taking action if a clearance is required. Until the Security Manager has approved the requirement for a clearance no action will be taken (Figure 3-D). CPD will initiate appropriate paperwork for investigation and eventually prepare the clearance certificate (OPNAV 5520/20).

NOTE: Keep in mind the number of clearances per department has already been established and restricted; clearances are extremely limited and controlled.

4. Clearance and Access Listing. The Command Security Manager will promulgate a semi-annual directive containing a listing of personnel, military and civilian, and their clearance for and access to classified information. This information will be promulgated to security coordinators for their reference, review and update.

3-6 Certificate of Clearance. The Certificate of Personnel Security Investigation, Clearance and Access (OPNAV 5520/20) is a permanent part of an individual's service record. Once an individual is issued a certificate of personnel security clearance and the investigation remains valid in accordance with OPNAVINST 5510.1, it serves as a valid basis for access to classified material at subsequent departments and Navy commands without the issuance of a new certificate, provided any adverse information which becomes known subsequent to issuance of a clearance is favorably resolved, or there is no break in service greater than one year.

3-7 Classified Information Non-Disclosure Agreement (SF-189). Before being granted access to classified material, the Commanding Officer must ensure that personnel under their jurisdiction are briefed and have executed a Classified Information Non-Disclosure Agreement (SF-189) Figure 3-E.

1. The SF-189 needs only to be executed once. A local record of its execution is kept, the original forwarded to NSIC (Code 29), and an annotation made in the comments section of the OPNAV 5520/20 denoting the fact.

2. If prior execution of an SF-189 cannot be verified, another one should be completed.

3. Since the SF-189 is a contractual agreement between the individual granted access and the U.S. Government, the only individuals authorized to witness the signature are the CO, XO or the Command Security Manager.

4. The date of execution and witness date must be the same.

3-8 Termination of Personnel Security Clearances/Access

1. Personnel security clearances/access can be administratively withdrawn where there is no foreseeable need for continued access to classified information or material in connection with the performance of official duties. A security clearance/access may also be revoked for cause when it is determined in compliance with due process of law that a person holding such clearance/access is no longer reliable or trustworthy. The general requirement for such actions are listed in OPNAVINST 5510.1, paragraph 22-5.

2. Requests for initiating procedures to revoke a security clearance/access shall be made by the department head, in writing, to the Commanding Officer via the Command Security Manager.

3-9 Security Termination Statements

1. A Security Termination Statement (OPNAV 5511/14)(Figure 3-F) will be obtained from the following categories of persons prior to their separation.

a. Civilian personnel being retired, resigning from Federal Service or on temporary separation of more than 60 days, including sabbaticals and leave without pay.

b. Military personnel being retired, released from active duty or discharged.

c. All personnel when their clearance is revoked for cause or administratively withdrawn.

20 JUL 1987'

2. The security termination statement will be executed by the Assistant Security Manager (Admin Support Services Supervisor) for military personnel and the department security coordinator for civilians. All Security Termination Statements will be filed in the individual's official record and a copy retained by the command for two years.

3-10 Administrative Withdrawal. A clearance will be administratively withdrawn when current duties do not require access to classified material. It may never be withdrawn for cause.

1. The OPNAV 5520/20 will be annotated to show that action was taken administratively and without prejudice to future eligibility for access. The original will be retained in the official personnel record with a copy sent to NMPC.

2. The individual should be debriefed and a security termination statement executed and filed in the official personnel record.

3. When an immigrant alien does not become naturalized, a clearance will be administratively withdrawn.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement: Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) that granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold, removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made me aware of Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.
11. I have signed this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)
ORGANIZATION		

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE
ORGANIZATION	

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.
11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)
ORGANIZATION		

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE
ORGANIZATION	

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.

CHAPTER IV
SECURITY VIOLATIONS

(COMPROMISE OF CLASSIFIED INFORMATION)

4-1 Definition and Policy. "Security violation" as used in this instruction refers to any failure to comply with the regulations relative to the security of classified material.

1. NAS Oceana personnel are individually responsible for ensuring that knowledge of classified information which becomes available to them by any means is revealed only to persons who have been properly cleared and who have a "need-to-know". Although a security violation may be the result of carelessness rather than a willful disregard of security measures, the effect is no less serious.

2. Individuals found responsible for the loss, unauthorized disclosure or possible subject to compromise of classified information through non-compliance with directives pertaining to the safeguarding of classified information may be subject to disciplinary actions.

4-2 Reporting Violations (Possibility of Compromise)

1. Persons having knowledge of the possible loss, compromise or unauthorized disclosure of classified information or other violations of security (deliberate or inadvertent) shall immediately report the facts to the Commanding Officer via the Command Security Manager on a NAS Oceana Form 5510/3. The Commanding Officer will direct a preliminary inquiry and, should circumstances warrant, a follow-on JAG investigation.

2. All security violation reports will be completed on NAS Oceana Form 5510/3 (See Figure 4-A).

4-3 Processing Violations

1. All security violation reports (NAS Oceana Form 5510/3) will be processed by the Command Security Manager after receipt of the completed violation report, which will include department head recommendations for disposition of the violation.

2. The completed violation report must reach the Command Security Manager by 1200 hours on the day following the reported violation.

4-4 Preliminary Inquiry/Investigation/JAG Manual Investigation

1. A preliminary inquiry is to determine if unauthorized disclosure of classified material did or did not occur, that compromise may have occurred, but under conditions of minimal risk to national security, that compromise is confirmed or that the probability of identifiable damage to the national security cannot be discounted. When the preliminary inquiry determines that a compromise has occurred with probable damage to the national security, reveals significant security weakness, or determines that disciplinary action is appropriate, a JAG Manual investigation must be conducted. When directed by letter, the investigating officer shall:

a. Identify completely and accurately the compromised information, to include the following:

- (1) Classification.
- (2) Identification and/or serial numbers.
- (3) Originator.
- (4) Subject or equipment function.
- (5) Date of material.
- (6) Downgrading and declassification instructions.
- (7) In case of documents, total number of pages involved.

b. Identify all witnesses to the violation.

(1) Informally conduct an interview to the extent necessary to determine the circumstances of the violation. The results of this investigation will establish either:

(a) That an unauthorized disclosure of classified information did not occur or that compromise may have occurred but under conditions of minimum risk to national security.

(b) That compromise is confirmed, or probability of identifiable damage cannot be discounted.

2. A JAG investigation shall be conducted when:

a. The preliminary inquiry indicates that further investigation is necessary.

b. Directed by higher authority. Security violations involving COMSEC (CMS) information will be handled in accordance with CMS-4.

3. The Security Manager shall:

a. Keep the Commanding Officer and Executive Officer advised on the status of all security violations and corrective action being taken.

b. Closely follow the progress on all preliminary inquiries and JAG investigations, providing assistance as necessary.

4. The investigating officers shall:

a. Conduct preliminary inquiries and/or JAG investigations expeditiously and in accordance with OPNAVINST 5510.1 (series), CMS-4, and the JAG Manual, as applicable. Preliminary inquiries will be completed in three working days.

b. Consult with the Command Security Manager as necessary for interpretation of security regulations and command procedures. NIS and the Staff Judge Advocate should also be consulted as necessary for further clarification of security regulations and legal procedures. Duties as an investigating officer, preliminary or JAG, will take precedence over normal duties assigned.

5. Security violation reports will be submitted to higher authority in accordance with OPNAVINST 5510.1 (series) and CMS-4 as applicable. The Command Security Manager will be responsible for the initiation of command reports or responses to security violations for the Commanding Officer's approval and release. The CMS Custodian will initiate reports on COMSEC violations for the Command Security Manager's review and the Commanding Officer's approval and release.

4-5 Security Discrepancies

1. A security discrepancy is defined as an administrative or clerical error involving classification markings and/or downgrading/declassification instructions. Receipt of a classified document with incorrect, improperly placed markings or missing downgrading/declassification instruction requires the following response:

a. The Assistant Security Manager (Admin Support Services Supervisor) will complete and mail to sender a Security Discrepancy Notice, OPNAV 5511/51.

b. Mail a copy of the Security Discrepancy Notice to CNO (OP-009D). The copy of the OPNAV 5511/51 sent to CNO (OP-009D) requires only the name of the reporting command. The To line and the Reference (a) line may be obliterated.

c. Properly mark the document in accordance with OPNAVINST 5510.1 series.

4-6 Inspection of Spaces

1. Security inspections of NAS Oceana spaces will be conducted periodically by the Command Security Manager and other designated security personnel.

- a. A Security Violation Report, NAS Oceana Form 5510/3, shall be issued for each violation or discrepancy.
- b. The Command Security Manager shall be notified immediately of all violations deemed to be of a serious or complex nature.

20 JUL 1987

JAG MANUAL INVESTIGATION CHECKLIST

In review of JAG Manual investigations, the following points should be considered.

1. Were the originators of the material notified by report of preliminary inquiry? Was the chain of command? CNO (OP-009D)?
2. Was there a requirement to report to Naval Investigative Service? Has it been done?
3. Was the initial opinion of probability of compromise logical?
4. Was a JAG Manual investigation necessary? Was the proper investigative body convened?
5. Were there sufficient grounds for any long delay in investigation?
6. Have interested parties been designated? Is designation of interested parties allowed under the type of investigation convened? Were they afforded the rights of a party?
7. Are findings of fact supported by evidence? Are they facts rather than opinions?
8. Do the findings of fact include:
 - a. Complete identification of the material?
 - b. Adequate identification of the individuals mentioned in the report?
 - c. Chronology of circumstances relating to the event?
9. Are all opinions supported by evidence or logically drawn from findings of fact?
10. Has a time frame been established during which the material was subjected to compromise?
11. Is individual culpability indicated but not assigned?
12. Is the degree of probability of compromise logically drawn from findings of fact/opinions?
13. Have weaknesses in security procedures been recognized?
14. Have recommendations been made as to remedial action?
15. Has disciplinary action been taken? If punitive, was the legal basis present? (Designation as an interested party, impartial hearing under UCMJ, or proper administrative procedures for civilians.) Does disciplinary action taken or recommended fit the culpability?
16. Has investigation been forwarded through the chain of command?
17. Have endorsers made recommendations to be acted upon subordinates? By those in the chain of command? By CNO?
18. Have originators been provided with copies of the investigation?

CHAPTER V

ACCOUNTABILITY AND CONTROL

5-1 General. This chapter provides procedures and guidance in addition to the general requirements of OPNAVINST 5510.1 (series) for the accountability and control of all classified material received and generated by Naval Air Station Oceana. All classified material records are under the control of the Command Security Manager and all such material will be recorded and accounted for as outlined in this chapter.

5-2 Classified Material Control Points

1. All classified material received by an activity is accountable. The Command Security Manager maintains the recording accountability and disposition records of all classified material in conjunction with the following secondary control points:

- a. Top Secret - Top Secret Control Officer
- b. Communications Material Systems - CMS Custodian
- c. Naval Warfare Publications - NWPL Custodian
- d. Classified Equipment/Parts - AIMD Officer or Supply Officer
- e. Secret/Confidential Correspondence - Assistant Security Manager (Admin Support Services Supervisor)
- f. Secret/Confidential - Assistant Security Manager (Admin Support Services Supervisor)
- g. Department Level Classified Material - Department Security Coordinator/
Departmental Custodian

2. The Administrative Department's Postal Clerk will receive all official mail for the command. He/she will record all registered mail in the Registered Mail Log. (This log will be periodically audited by Internal Review to ensure proper chain of custody.)

a. The postal clerk will deliver all registered material for NAS Oceana to the Admin Support Services Supervisor. It will be opened to determine if classified.

b. If classified, the Admin Support Services Supervisor will retain and sign the registered mail log for receipt.

c. If not classified, the postal clerk will have the appropriate department accept and sign a receipt for the material.

d. The classified material will be entered into the accountability system by the Admin Support Services Supervisor.

(1) All material to be retained in the Admin files will be page checked by the Admin Support Services Supervisor and the enclosed record of receipt card returned (sent with secret material).

(2) A Correspondence/Material Control Form (MCF), OPNAV Form 5216/10, Figure 5-A will be prepared.

(3) If a discrepancy exists, the Command Security Manager will be advised and appropriate steps to report the discrepancy will be initiated.

3. The Administrative Incoming Correspondence Clerk will open all regular mail received at the command to determine if it contains confidential material. All confidential material will be delivered immediately to the Admin Support Services Supervisor for proper control and routing. An MCF will be prepared and appropriate routing assigned.

20 JUL 1987

5-3 Correspondence/Material Control Form (MCF), OPNAV Form 5216/10. The MCF (OPNAV 5216/10) will be filled out as follows:

1. An Activity Control Number (ACN) will be assigned to each document.
 - a. ACNs will be sequentially assigned and will appear on the Material Control Form (top and bottom) and on the document itself.
 - b. ACN series will be assigned by calendar year to each classification in the following manner:

TS0001-(YR)	Top Secret
S001-(YR)	Secret
C01-(YR)	Confidential
 - c. Multiple copies of classified documents shall be assigned with a copy number added (that is, S001-87 copy 1 of 3, S001-87 copy 2 of 3, S001-87 copy 3 of 3 and so forth).
2. The following information shall be completely entered on the MCF (OPNAV Form 5216/10)
 - a. Classification of MCF (top and bottom).
 - b. Classification of material.
 - c. Originator.
 - d. Originator's serial number.
 - e. Date of material.
 - f. File Symbol Number (SSIC)
 - g. Cross reference (enter registered mail number).
 - h. Date material received.
 - i. Reply due date (assign due date if action classified correspondence).
 - j. Addressee.
 - k. Number of copies received.
 - l. Subject (unclassified).
 - m. All enclosures (if no enclosures, type NONE in this block; include classification).
 - n. Routing sequence (assigned by Admin Support Supervisor and approved by the Command Security Manager).
 - o. The reverse side of the original MCF will show the inventory stamp, verifying the inventories conducted (Figure 5-B).
3. The original and first flimsy copy sheet will be attached to the document for routing to XO, CO and to departments for information.
4. The second flimsy copy will be placed on a clipboard in order to track routing and serve as a tickler.
5. The hard copy card of the four-part MCF will serve as the top secret, secret and confidential inventory log. (Effective July 1987; prior to this date the log will consist of a flimsy copy of OPNAV 5511/23 series, with signatures, and will be filed sequentially by classification and year received in a looseleaf binder, file folder or a two-post clipboard.)

6. The MCF shall be retained for at least two years following destruction of the classified material to which they pertain.

5-4 Control and Routing

1. The Admin Support Services Supervisor will contact the appropriate department within one working day of receipt of classified material. The departmental custodian/security coordinator will report to Admin to accept custody of material immediately. He/she will page check all material, sign and return the enclosed Record of Receipt Card (sent with secret material). Should any discrepancies be found, the Admin Support Services Supervisor will retain control and take appropriate steps to report any discrepancy and advise the Command Security Manager. If the incoming classified material is found to be complete, the departmental custodian/security coordinator will sign the original OPNAV Form 5216/10 receiving custody of the material. The first flimsy will remain attached to the material.

2. The following is guidance for specific control of classified material.

a. Top Secret Material

(1) Material shall be properly identified by classification and marking. A top Secret Cover Sheet (Standard Form 703) will be attached to all top secret material.

(2) A specifically designated safe is provided and appropriately coded for storage of top secret material. Only the Top Secret Control Officer and designated assistant(s) shall be authorized access to the safe combination and contents therein. Top Secret CMS distributed material shall be stowed and accounted for by the CMS Custodian in accordance with CMS-4. The "two-man rule" applies to all Top Secret material handling' i.e. no one person may handle Top Secret alone.

(3) A record of receipt or origination shall be maintained on an OPNAV Form 5216/10 and will include:

(a) Identification of the document including changes thereto.

(b) The number of copies and disposition of each.

(c) Assigned top secret control number

(d) Record of page check: annually, upon initial receipt, upon entering a change and upon change of custodian.

(4) Internal dissemination procedures shall include:

(a) An affirmative determination that the individual is cleared and has a need-to-know before providing access to material.

(b) Hand-to-hand transfer/routing by the Top Secret Control Officer or designated assistant.

(c) A disclosure record (OPNAV Form 5511.13) retained with each top secret item.

(d) A signed receipt or copy (OPNAV Form 5510/10) for each top secret document received and/or transmitted by the command.

(5) Top secret material shall not be reproduced without the consent of the originating agency or higher authority. All requests must be sent via the Commanding Officer.

(6) An inventory of all top secret material, except CMS distributed, shall be conducted annually by the Top Secret Control Officer or designated assistant, with a written report to the Commanding Officer via the Command Security Manager.

(7) A record of transfer of accountability to another command shall be maintained.

20 JUL 1987

(8) Disposition and/or destruction of top secret material shall be conducted as authorized by the originating agency or higher authority and certified as directed. A Classified Material Destruction Report (OPNAV Form 5511/12) shall be utilized to record destruction.

b. Secret Material. All secret material received by registered mail or hand carried into the command is to be logged in and controlled by the Admin Support Services Supervisor. Steps for controlling secret material within the command are as follows:

(1) The package will be checked for completeness and a record of receipt (OPNAV 5511/10) will be signed by the authorized classified custodian/security coordinator and returned to the sender.

(2) A Secret Cover Sheet (Standard Form 704) will be attached and the material assigned a sequential control number, which is entered on the face of the document.

(3) An MCF will be completely filled out and attached in accordance with section 5-3 of this chapter.

(4) All secret material will be signed for by the department custodian/security coordinator.

(5) Secret material is not to be hand carried from one department to another. When a classified document has completed routing in one department, it will be returned to the Admin Support Services Supervisor for further routing and positive control.

(6) Secret material, in routing for information, should not stay in any one department longer than three working days. The Admin Support Services Supervisor must be promptly notified when routing will require retention of material in excess of this time.

(7) Secret material required to be retained by a department must be signed for by the department custodian prior to subcustody and release by the Admin Support Services Supervisor. All department custodians must subcustody secret material from the Admin Support Services Supervisor. Retention requirements may be indicated by marking the attached control form MCF (upon completion of routing).

(8) The final decision for retention of secret material will be made by the Command Security Manager or higher authority. Due to the limited number of copies received in the command, distribution will be on a required and "need-to-know" basis.

(9) Provisions for reproduction of secret material are outlined in Section 5-6 of this chapter.

(10) A report of destruction of secret material or transfer from one departmental custodian to another must be accomplished through the Admin Support Services Supervisor to ensure proper accountability.

(11) Responsibility for control and signature custody is placed on the department security coordinator/departmental custodian. They will ensure the following actions:

(a) All secret material entering or leaving their department is logged on NAS Oceana Form 5511/1 (Figure 5-C).

(b) The OPNAV 5216/10 second flimsy is retained when material is routed within the department or sub-custodied within the department. Ensure that inter-departmental custody is entered on the first and second flimsies and signatures are obtained on the OPNAV Form 5216/10.

(c) The first flimsy is to remain on the material.

(12) All outgoing secret material for the command must be delivered to the Assistant Security Manager for processing. (Exception: Secret equipment or parts handled by AIMD/Supply.)

20 JUL 1987

c. Confidential Material. Procedures for the protection of confidential material are normally less stringent than those for secret; however, due to the size of this command the same administrative provisions for access control are required to protect confidential information from unauthorized disclosure as specified for secret in this instruction and in compliance with the regulations on markings, storage, transmission and destruction.

(1) All confidential material received by mail or hand carried into the command is to be logged in and controlled by the Admin Support Services Supervisor.

(2) Upon receipt of confidential material a Confidential Cover Sheet (Standard Form 705) will be attached.

(3) An MCF (OPNAV Form 5216/10) will be completed as directed in section 5-3 of this instruction. The same rules discussed under section 5-4 for handling secret material control and routing apply to confidential material at NAS Oceana.

(4) It will be checked for completeness. The department retaining custody of the material will fill out and return a Record of Receipt (OPNAV Form 5511/10), if attached.

(5) Provisions for reproduction of confidential material are outlined in Section 5-6 of this Chapter.

(6) A report of destruction of confidential material or transfer from one department custodian to another must be accomplished through the Admin Support Services Supervisor.

3. The establishment of record control procedures for all classified material introduced into NAS Oceana is vital. The following will apply:

a. All mail that is delivered to the Administrative Support Services Office will be carefully screened to ensure that all classified material is adequately protected and appropriately routed.

b. All classified material that is hand carried into the command by individual personnel or delivered to the department without being processed through the appropriate control point will immediately be taken to the Administrative Support Services Office for proper logging and accountability procedures.

5-5 Inventories of Classified Material. A command inventory of all classified material within NAS Oceana will be conducted at least annually, in August, upon transfer of the designated custodian, upon change of command or when other circumstances warrant. A report of department inventories will be submitted to the Commanding Officer via the Command Security Manager by 31 July. Individual custodians will maintain complete inventory records on NAS Oceana Form 5511/1 of all classified material held in their security containers. (A separate sheet, (NAS OCEANA Form 5511/2) will be placed within each drawer of the container in case of emergency destruction (Figure 5-D). A monthly inventory is highly recommended for personal use of department custodians. Classified material that has been lost, misplaced, inadvertently destroyed or classified material found adrift shall be reported to the Command Security Manager immediately.

5-6 Reproduction of Classified Information. The reproduction of classified material will be kept at an absolute minimum and approved only when absolutely required. Under no circumstances will individuals reproduce any classified material without prior approval by the appropriate control point. All classified material, including reproduced copies, must be entered into the NAS Oceana accountability system.

1. Reproduction Procedures. The Command Security Manager must approve the reproduction of all secret material. A memorandum must be submitted along with the material to be reproduced to the Command Security Manager. The requestor will be notified when material is ready for pick-up. Individuals are not authorized to personally reproduce classified material at any time without approval.

a. If approval for reproduction of secret material is given, such material will be reproduced and controlled by the Assistant Security Manager. Secret material will not be reproduced on "fast copy" equipment.

b. Confidential reproduction may be accomplished on any approved "fast copying machines" within the command, after approval is obtained through department security coordinator. Material may be reproduced by machines which have been designated by the Command Security Manager for reproduction, providing safeguards are taken to destroy all residue and control of the material is continuously maintained.

c. Department security coordinators/custodians will ensure a log is maintained to record all confidential material reproduced within the department. The log shall include the division/office copying the material, date copied, classification, unclassified description, number of copies reproduced and by whom reproduction was authorized. The department/office security coordinator is responsible for reviewing the log monthly.

2. Requests for reproduction of all top secret material must be made to the Commanding Officer via the Command Security Manager. Top secret material may not be reproduced without the specific authorization of the issuing office or higher authority, and must be controlled by the Top Secret Control Officer.

3. All reproduced material must be marked as "REPRODUCED" and indicate the date of reproduction. This material must contain all classified markings.

4. Overruns and spoilage material shall be handled and safeguarded as classified waste and destroyed promptly as classified waste.

5. The Command Security manager will maintain an inventory of all reproduction machines designated for the reproduction of classified material. Signs shall be posted in the area indicating the highest level of classified material to be reproduced on that machine (Figure 5-E and 5-F).

6. All reproduction machines should be located in areas that are easily observed to ensure that only authorized copies are being made and the number of copies is kept to a minimum.

SECURITY TERMINATION STATEMENT

OPNAV 5511/14 (REV. 7-78)
S/N 0107-LF-055-1171

20 JUL 1987
Enter name and address of appropriate Naval or Marine Corps activity obtaining statement.

1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (CMS-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.

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

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

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

5. I, _____, have been informed and am aware that Title 18 U.S.C. Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand appendix F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.

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

SIGNATURE OF WITNESS

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

TYPE OR PRINT NAME OF WITNESS

DATE

FIGURE 3-F

n-14564

WARNING

**THIS EQUIPMENT IS AUTHORIZED FOR REPRODUCTION
OF UNCLASSIFIED AND CONFIDENTIAL
MATERIAL ONLY!**

RULES FOR USE

- **REPRODUCTION OF SECRET/TOP SECRET MATERIAL IS PROHIBITED WITHOUT THE APPROVAL OF THE SECRET/TOP SECRET CONTROL OFFICER(S).**
- **REPRODUCE ONLY THE NUMBER OF COPIES AUTHORIZED FOR OFFICIAL PURPOSES.**
- **DO NOT ALLOW UNAUTHORIZED PERSONNEL ACCESS TO CLASSIFIED MATERIAL.**
- **UPON COMPLETION, REMOVE ALL CLASSIFIED MATERIAL FROM THIS MACHINE AND AREA.**
- **ENTER ALL CLASSIFIED MATERIAL REQUIRING RECEIPT INTO ACCOUNTABILITY RECORDS.**
- **INSURE IMAGE CARRYING PARTS ARE CLEARED AFTER REPRODUCTION OR BEFORE REPAIRMAN IS GIVEN ACCESS.**

COMMAND SECURITY MANAGER

WARNING

**THIS MACHINE DESIGNED FOR
UNCLASSIFIED REPRODUCTIONS ONLY**

**DO NOT USE
THIS MACHINE
FOR
CLASSIFIED
REPRODUCTION**

20 JUL 1987

CHAPTER VI

STORAGE

6-1 Responsibility. Whenever classified material is not in actual use or under immediate surveillance by an authorized person, it shall be the responsibility of the individual having custody to secure such material in a General Services Administration (GSA) approved security container in the manner set forth in this chapter.

6-2 Stowage Containers. Classified information in the custody of NAS Oceana shall be protected by stowage in secure equipment, specifically, GSA-approved security containers only, certified to be at the appropriate level. IN NO INSTANCE will classified material be secured in desks or cabinets. As a minimum, classified material will be stowed as follows:

1. Top Secret. Top Secret material will be stowed in a safe or safe-type steel file container having a built-in, three-position, dial-type combination lock as approved by GSA. All Top Secret material within this command will be held and filed only by the Top Secret Control Officer.
2. Secret or Confidential. Secret or Confidential material will be stowed in the same manner as Top Secret or in a steel filing cabinet equipped with a steel lock bar to prevent the opening of any drawer when the lock bar is inserted through all the keepers and is secured by an approved three-position, dial-type, combination padlock rated R or IR.
3. For Official Use Only. For Official Use Only material will be stored in a locked container, such as a file cabinet.

6-3 Location and Maintenance of Security Containers

1. Security containers may not be relocated without first informing the Command Security Manager.
2. Any malfunction of any security container will be reported immediately to the Command Security Manager by the custodian of the container. The Command Security Manager will advise the custodian of the appropriate action to be taken.

6-4 Combinations

1. It is essential that combinations be known only by those persons whose official duties require them to have access to the security container. Generally, this would include the custodian, alternate custodian and/or other persons who would normally require access during the custodian's absence.
2. Combinations to security containers equipped with built-in manipulation-resistant locks and padlocks, regardless of the classification of material stowed therein, shall be maintained by the Command Security Manager. Whenever a combination is changed, the container custodian will submit the new combination, sealed in a GSA Standard Form 700 (Figure 6-A) envelope, to the Command Security Manager for retention. The front of the envelope will be completely filled in. Part 1 will be attached to the inside of the locking drawer. The date the combination was changed must be indicated in the appropriate block. The container number block will include the department container number.
 - a. Record each combination on the Security Container Information Form, GSA Standard Form 700, copy 2. After completion, enclose copy 2 with the envelope. After sealing the envelope, mark the envelope with the appropriate classification (highest level of material stored in container).
 - b. Hand carry combination change envelope(s) to the Command Security Manager on the same day the safe combination is changed.

20 JUL 1987

c. Copy 1 of OPNAV 5511/30 will contain the names of the custodian/alternate custodians and shall be affixed to the outside top drawer of the container (see Figure 6-B). Copy 1 of GSA Standard Form 700 with home telephone numbers and home addresses of the custodians will be placed inside the locking drawer of the container. A privacy act statement will be provided to those listed. If a person refuses to provide his/her home address and home telephone number, that person cannot be the custodian of a security container (see Figure 6-C).

d. Any document showing the combination to a safe shall be classified in accordance with the highest classification of material in the container.

3. Combinations shall be dialed in a manner which prevents observation by unauthorized persons.

4. Combinations will be released by the Command Security Manager only upon official request by the custodian listed on the change envelope or by higher authority upon valid justification by the department head.

6-5 Combination Changes

1. All combination changes will be accomplished only by the Public Works Department authorized locksmith and the record of combinations will be maintained by the Command Security Manager.

2. The combination to security containers or padlocks shall be changed under any of the following circumstances:

a. When the container or padlock is initially received.

b. At the time any person having knowledge of it leaves the organizational unit.

c. At any time there is reason to believe it or the record of combination has been compromised.

d. Combination locks left in an unlocked condition and not under continuous surveillance must be changed before they are used again to protect classified information.

3. The same combination will not be used for more than one container in any one component.

4. In selecting combination numbers, multiples of 5, simple ascending or descending arithmetical series and personal data such as birth dates and serial numbers should be avoided.

5. In setting a combination, numbers that are widely separated will be used. This can be achieved by dividing the dial into three parts and using a number from each third as one of the combination numbers.

6. To prevent a lockout, a new combination should be tried at least three times before closing the container, preferably by two different individuals.

6-6 Safe or Cabinet Security Record. Each custodian of a classified security stowage container will affix a copy of GSA Standard Form 702 to each container. When a container is unlocked, the DATE, INITIALS and TIME columns will be completed by the individual who opens the container. Whenever the container is locked the CLOSED BY and CHECKED BY columns must be individually initialed by two separate individuals. The only exception to initialing the CHECKED BY for a locked container by two separate individuals is when a late worker is working alone and no one else is available to check the container. If the container is opened and locked more than once each day, the next line on the form will be used. No more than one set of initials shall appear in any one space on the form (see Figure 6-D).

6-7 Equipment Records Management. In order that all security storage containers, storage cabinets, safes or other equipment used for security purposes within the command are properly utilized for their designated purpose and to establish an effective equipment records manage-

20 JUL 1987

ment program, OPNAV Form 5510/21 (Security Container Records Form) will be completed on such equipment maintained (one card for each piece of equipment) and forwarded to the Command Security Manager. Updated information will be forwarded as required when changes, modification or transfer of the equipment is effected (see Figure 6-E).

6-8 Equipment Types and Specifications

1. Reference (a) specifies that only security filing cabinets that have been approved by the Federal Government shall be procured whenever new equipment is needed, and further, it prohibits new modification of existing filing cabinets to a lockbar/padlock variety when such a modification is intended to provide a means for the storage of classified material.

2. This requirement will eventually result in the replacement of all nonapproved containers for classified material storage by containers designed as security filing cabinets.

3. The Command Security Manager will assist in the selection of equipment. Department heads should consider the following:

a. When new security equipment is selected, emphasis will be given to the threat, location and supporting security measures in effect as well as to the amount and type of material to be safeguarded; and, within a department, the best containers should be used to protect the most sensitive material. The Security Container Records Form (OPNAV Form 5510/21) discussed in this instruction provides a means to conduct periodic review of container contents through which effective container usage may be achieved base-wide.

6-9 Storage of Classified Equipment/Parts. The Supply and AIMD officers are tasked with developing plans for the control and secure storage of classified equipment/parts in accordance with maintenance and supply directives and in accordance with the intent of reference (a) and this instruction.

6-10 Stowage Responsibilities of Custodians

1. Ensure that each vault or container used for the storage of classified material is so designated and contains a security container number assigned by the department with a copy to the Command Security Manager.

2. Ensure that safe or vault combinations are changed as required and that necessary reports to this effect are promptly made to the Command Security Manager.

3. Ensure that each vault or container that is used for the stowage of classified information has posted thereon, in a conspicuous place, a form containing the name of the primary and alternate custodian who are responsible for the container and its contents. This information will be kept up-to-date at all times. OPNAV Form 5511/30 shall be used for this purpose.

4. Ensure that each vault or container that is used for the stowage of classified information has posted on the inside Part 1 of GSA Standard Form 700, containing the name, address and telephone number of each person who has the container combination. Copy 2 is placed in an envelope, sealed, marked with appropriate classification and hand carried to the Command Security Manager.

5. Ensure that each vault or container that is used for the stowage of classified information has affixed thereon in a conspicuous place a copy of the Security Container Check Sheet (SF Form 702) (Figure 6-D). This form will be completed by the primary or alternate custodian each time the container is opened or secured. The form will be replaced when full and will be kept current.

6. At least once annually, inspect all departmental security containers to ensure that they are in good repair and that the safeguarding features of the containers are effective. Report the results of this inspection to the Command Security Manager by memorandum.

7. Carry out such other responsibilities concerning safeguarding and control of classified information as required by the department director or higher authority.

20 JUL 1987

6-11 Stowage Prohibitions. The stowage of money, jewels, precious metals and narcotics is prohibited in security containers used for storage of classified material.

6-12 Non-Classified Stowage. A tag on each desk, file or cabinet will state that the equipment contains no classified information. The custodian of the desk, file or cabinet will sign the statement. (See Figure 6-F). Classification labels are not to be fixed to the exterior of cabinets, card trays, card drawers or security containers that do contain classified material.

SECURITY CONTAINER INFORMATION INSTRUCTIONS		1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).		4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.		6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.		9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		
4. DETACH PART 2A AND INSERT IN ENVELOPE.		10. Immediately notify one of the following persons, if this container is found open and unattended.		
5. SEE PRIVACY ACT STATEMENT ON REVERSE.		EMPLOYEE NAME		
		HOME ADDRESS		
		HOME PHONE		

1. ATTACH TO INSIDE OF CONTAINER 700-101
NSN 7540-01-214-5372 **STANDARD FORM 700 (8-85)**
Prescribed by GSA/ISOO
32 CFR 2003

WARNING
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____
 _____ turns to the (Right) (Left) stop at _____

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED

UNCLASSIFIED UPON CHANGE OF COMBINATION

2A INSERT IN ENVELOPE

SF 700 (8-85)
Prescribed by
GSA/ISOO
32 CFR 2003

CHAPTER VII
SAFEGUARDING

7-1 Custodial Responsibilities

1. Personnel at NAS Oceana are individually responsible for ensuring that classified information which they prepare, receive, sign for or handle is properly accounted for and is made available only to persons who have an appropriate security clearance and for whom a legitimate "need to know" has been clearly established.

2. Personnel shall not remove classified material from the physical confines of NAS Oceana spaces without the knowledge and approval of the cognizant Department Head and an authorization from the Command Security Manager. A complete list of the removed material shall be prepared by the individual removing the material and given to the Command Security Manager. Under no condition shall classified material be removed to an individual's residence. Procedures for hand carrying classified material are contained in Chapter VIII of this plan.

3. A custodian and an alternate shall be designated for each container used for the stowage of classified information aboard NAS Oceana. Classified Container Information Form OPNAV 5511/30 and Security Container Information Form GSA Standard Form 700 will be used. Custodians must possess valid security clearances for the highest category of information stowed. Custodians shall have primary responsibility for compliance with all the security procedures relating to the container and its contents.

a. The classification of the material shall not be indicated on the outside of the container.

b. A complete inventory of classified material, NAS Oceana Form 5511/1, will be used (see Figure 5-C). Chapter 5 of this plan provides guidance in accountability. A monthly inventory is recommended.

c. Message traffic should be separated from letter correspondence at least by a separate folder.

d. Classified publications should be kept in a separate drawer.

e. NATO classified material shall be separated from U.S. classified even if they are the same level of classification.

f. Attention should be paid to declassification dates of stored material.

g. All material or material folders will be color coded to indicate the classification of material contained therein. In addition, destruction of classified material shall be carried out in the priority listed.

(1) BLUE - FIRST PRIORITY - COMSEC material marked TOP SECRET (detailed information concerning the order of destruction of COMSEC material is contained in the effective editions of KAG-1 and CMS-4).

(2) RED - SECOND PRIORITY - U.S. TOP SECRET MATERIAL.

(3) WHITE - THIRD PRIORITY - COMSEC MATERIAL MARKED SECRET.

(4) YELLOW - FOURTH PRIORITY - U.S. SECRET MATERIAL.

(5) GREEN - FIFTH PRIORITY - U.S. CONFIDENTIAL MATERIAL AND NATO MATERIAL.

7-2 Care During Working Hours

1. Individuals shall exercise every precaution to prevent access to classified information by unauthorized persons. The following precautions apply:

- a. Classified documents removed from stowage for working purposes shall be kept under constant surveillance and covered when not in use.
- b. File drawers and other containers of classified material shall be closed when not in use.
- c. Classified information shall never be discussed over the telephone, in corridors, restaurants or in public conveyances.
- d. Do not record combinations to classified containers on telephone indexes, calendars, etc.
- e. Preliminary drafts, carbon sheets, carbon tape typewriter ribbons (one-time), plates, stencils, stenographic notes, worksheets and all similar items containing classified information shall be destroyed immediately after they have served their purpose or shall be given the same classification and safeguarded in the same manner as the classified information produced from them.
- f. Never place classified material in your desk.
- g. All fabric typewriter ribbons may be treated as unclassified after the ribbon has been cycled through the typewriter at least five times. Carbon and plastic typewriter ribbons used in production of classified material will require removal from the typewriter and stowage in a classified container pending destruction.
- h. In every instance, ribbons used to type top secret material shall be removed and turned in to the Top Secret Control Officer along with the material typed, scraps, roughs, etc.
- i. Classified mail from outside the command, which is addressed to or hand carried to an office directly, shall be delivered to the Admin Support Services Supervisor to be processed into the official accountability system (see Chapter V of this plan).
- j. If, for any reason, a room must be vacated during working hours, classified material therein must be secured in an approved stowage container. Under no circumstances will the room be left unattended or secured only with a key lock.

7-3 Care and Stowage After Working Hours. Prior to departing office spaces, each employee is responsible for ensuring that all classified material, including burn bags, has been properly stowed. The best method for accomplishing this is to practice the "clean desk" policy. All departments shall require a system of security checks and inspection at COB each day. Inspections shall be recorded and retained at least until the next formal security inspection is conducted. In the event of a stowage cabinet malfunction after hours, the custodian shall notify the Command Duty Officer and request assistance. Under no circumstances will classified material be abandoned due to lack of sufficient stowage facilities or left unattended during transfer to other facilities.

7-4 Securing for the Day Procedures

1. At the end of normal working hours, the following procedures will be observed:
 - a. All classified and For Official Use Only letters, manuals, cards or other papers will be cleared from desk tops, file tops, cabinet tops and floors before securing for the day.
 - b. Bulky unclassified material, which is temporarily not stored within a container, will be marked conspicuously as "UNCLASSIFIED" and the name of the person responsible for it affixed.
 - c. Check all typewriters, terminals, fans/heaters, etc. to ensure that they are turned off.
 - d. Check all incoming and outgoing desk trays, desk tops and the general area for classified/privacy material inadvertently left unstowed.

20 JUL 1987

e. Check all wastepaper baskets for classified/privacy information and for used carbon paper, typewriter ribbons, dictating machine tapes, etc.

f. Burn bags will be stored as directed in accordance with paragraph 2-101.

g. The custodian of each container will record on the closure log (Security Container Check Sheet (SF 702) - Figure 6-D) the time that the container was locked. Re-check all safes and security containers to ensure that they are locked. Test each drawer by pulling the handle vigorously several times. Rotate the dial, in a clockwise direction ONLY, at least four complete revolutions. Retest the drawers.

h. When a security container is still open because the custodian/alternate is listed as an "exception" and is still present, the signing of the above Standard Form 702 is not required. This will be signed by the person conducting the second check after the custodian/alternate secures or by the custodian/alternate if he/she is the only one left in the area.

i. Personnel still in the area at the time of the security check will initial in the column for that day. The supervisor will advise the individual remaining in the area after the security check regarding the requirement to secure doors, windows, air conditions, fans and other equipment. The last person out ensures that all doors are locked and signs the Activity Security Checklist (Standard Form 701 - Figure 7-A) after conducting the second check of the entire area.

2. After Hours Personnel. All personnel who return to or report for work after normal working hours will assume security responsibility for those spaces and will make sure all equipment and lights are turned off, windows closed and exterior doors are locked. Procedures outlined in paragraph 1. above will also be followed. (All personnel who are not secured at the end of normal working hours are to be considered as "exceptions." Shift personnel are excluded. Personnel who work on shifts will conduct their check-out at the end of shift and exchange custodial responsibility to next shift as required.)

7-5 Care During Emergency. In the event of a fire or other emergency, classified material shall be stowed in the same manner as at the end of a working day, if possible. Each person possessing classified material at the time of an emergency shall make every effort to safeguard such material consistent with minimizing the risk of injury or loss of life. If return to the premises is possible, containers must be examined for damage or possible compromise. Possible compromise or loss will be reported to the NAS Oceana Security Manager as soon as possible.

7-6 Classified Material Found Unattended After Normal Hours. Any classified material found unattended or not properly stowed must be immediately locked in a security container to ensure proper safeguarding and note the security violation on the watch checklist. If a container in which classified material is stowed is found unlocked in the absence of assigned personnel, such information shall be reported immediately to the CDO. The container shall be guarded until the CDO arrives at the location of the unlocked container. The CDO shall then inspect the classified material involved and lock the container. If the CDO thinks the material may have been subjected to compromise, he/she will require the custodian or an alternate custodian to come and inventory the material. If it is felt that classified information may have been compromised, a detailed report shall be submitted to the Commanding Officer. In any case, the CDO will report violations to the Security Manager no later than the following working morning on NAS Oceana Form 5511/4 (Figure 4-A). The Security Manager will prepare necessary correspondence for the Commanding Officer's signature to ensure necessary administrative action is initiated, if required.

7-7 Telephones

1. Telephones will not be used to discuss classified information under any circumstances.
2. The use of the telecopier to transmit classified information is prohibited.
3. DOD telephones are provided for the transmission of official government information and are subject to communications security monitoring at all times. Use of official telephones constitutes consent to communications security monitoring in accordance with DOD Directive 4640.6.
4. Telephones will be answered "this is not a secure line" in areas where classified or sensitive information is discussed.

20 JUL 1987

CHAPTER VIII

TRANSMISSION

8-1 Basic Policy. Classified information will be transmitted either in the custody of an appropriately cleared and authorized individual or by an approved system or carrier, and in accordance with the provision of reference (a), Chapter 15.

8-2 Guard Mail. Classified material will not be included in guard mail envelopes or put in the guard mail system. Classified material will be covered and hand delivered to the appropriate control point or individual.

8-3 Regular Mail System. All classified material must be double-wrapped for transmission in the United States Postal system. This includes confidential material being transmitted by First Class mail. The following procedures are for transmitting classified material through the regular mail system:

1. Top Secret. All top secret material entering or leaving NAS Oceana must be transmitted through the Top Secret Control Officer.

2. Secret. Outgoing secret material shall be delivered with appropriately marked envelopes or mailing labels to the Assistant Security Manager (Admin Support Services Supervisor) for mailing from the command or for routing outside the originating group. Secret material shall be transmitted by United States Registered Mail. A Record of Receipt, OPNAV 5511/10 must be prepared for secret material.

a. When ready for release, outgoing correspondence attached to secret controlled material shall be delivered for clearance of accountability to the Assistant Security Manager.

b. When the correspondence is signed and ready to be released, the Assistant Security Manager will affix the date and serial number, attach receipts and ensure that classification markings, including downgrading and declassification marks, are affixed correctly prior to transmitting.

c. All secret material received within NAS Oceana must be processed immediately through the Assistant Security Manager (Admin Support Services Supervisor).

3. Confidential. Each code must prepare its own envelopes or mailing labels for mailing confidential material, then send it to the Administrative Postal Office for mailing.

a. U.S. Postal Service First Class mail shall be used to mail confidential material to Department of Defense (DOD) components located within the United States. Confidential material transmitted to DOD contractors or non-DOD agencies of the Executive Branch within the United States must be sent by certified mail. Confidential material sent first class or priority must have the warning on it: "POSTMASTER DO NOT FORWARD. RETURN TO SENDER."

Confidential mail to be sent first class, which is an "outsize" piece (over the 4" x 9 1/2" legal-size envelope), must be stamped FIRST CLASS. If a piece of confidential mail weighs over 12 ounces, it is to be marked PRIORITY MAIL.

b. U.S. Postal Service registered mail shall be used for transmitting confidential material to all FPO or APO addresses, to any addressee when the originator is uncertain that its location is within the United States and when the material is NATO information classified no higher than confidential.

8-4 Preparation of Envelopes or Containers

1. Envelopes. Whenever classified material is transmitted, it shall be enclosed in two opaque, sealed envelopes or similar wrappings, where size permits, except as provided in paragraph 2 below.

a. Classified written material shall be folded or packed so the text will not be in direct contact with the inner envelope or container.

20 JUL 1987

b. The inner envelope or container shall show the address of the receiving activity, highest classification of the material enclosed stamped in red and larger than other type on both sides in at least two places so that a portion of the stamp is on the tape and a portion is on the envelope. Include, where appropriate, the "Restricted Data" marking and any special instructions. It shall be carefully sealed with 3-inch wide filament reinforced gummed tape (MSN 8135-00-598-6097) to minimize the possibility of access without leaving evidence of tampering.

c. The outer envelope or container shall show the complete and correct address and the return address of the sender. The outer cover shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks which might invite special attention to the fact that the contents are classified. The outer cover of confidential material being transmitted by United States Postal Service first class mail shall be marked "FIRST CLASS" and endorsed, "Postmaster: Do Not Forward, Return to Sender."

2. Containers. Whenever the classified material being transmitted is too large to prepare as in paragraph 1 above, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings, or prepared as follows:

a. If the classified material is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure.

b. Material used for packaging shall be of such strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container. The wrappings shall conceal all classified characteristics. Packages shall be sealed with tape which will retain the impression of any postal stamp. Masking tape is not acceptable. Bulky packages shall be inspected by the Administrative Postal Clerk to determine whether the material is suitable for mailing or whether it should be transmitted by other approved means.

3. Addressing

a. Classified material shall be addressed to an official Government activity or DOD contractor and not to an individual.

b. Current issues of the Standard Navy Distribution List, Part 1 and 2, shall be consulted for complete and correct mailing addresses and mailing instructions.

8-5 Classified Material Received in a Damaged Condition/Improperly Received

1. When classified material is received in a damaged condition or shows evidence of having been tampered with, this fact shall be reported to the Command Security Manager or Assistant Security Manager and appropriate reports will be submitted to the sender by the Command Security Manager or Assistant Security Manager. Further investigation may be initiated if required.

2. When classified material is received not properly packed and transmitted, this fact shall be reported to the Command Security Manager who will initiate appropriate action.

8-6 Receipt Systems. Top secret material shall be transmitted under a continuous chain of receipts, while secret material shall be covered by a receipt between commands and other authorized addressees. A registered mail receipt does not satisfy that requirement. Registered mail merely acknowledges that a package was received; it does not assure the sender that each piece of secret material has been entered in the accountability system of the recipient. Until the sender of secret material gets that receipt, the sending command is considered to have custodial responsibility for reporting and investigating loss (or damage) in transit. When preparing classified material for forwarding, a Record of Receipt Card, OPNAV 5511/10, must be prepared. Record of Receipt Cards are to be checked weekly in order to initiate tracer action if the original receipt card is not received with 30 days. Accountability is not transferred until the recipient signs and returns the card to the sender.

8-7 Transmission by Other Than Regular Mail. The Transmission of top secret material other than through the top secret custodian is not authorized. Secret and confidential documents may be hand carried outside the command in conjunction with official business provided the following conditions are satisfied:

1. Serious impediment of a program or project would result if the material were not hand carried.

2. The necessary classified material is not available at the activity to be visited.
3. The time element will not permit transmission of the material by official U.S. Post Office Department channels or by an authorized courier service in advance of the visit.
4. The classified material shall be properly packaged and will not be opened, read, studied, displayed or used in any manner in public places or conveyances.
5. The classified material will be stowed in government approved facilities, except during the actual process of transporting the material. Prior arrangements will be made with appropriate offices, duty officers, etc., for temporary retention of the material when overnight storage incident to travel is required.

8-8 Courier Authorization Aboard NAS Oceana. Courier authorization is required for hand-carrying of classified material while on official business aboard NAS Oceana. A courier authorization card will be obtained from a department security coordinator prior to hand carrying classified material between buildings (NAS Oceana Form 5510/3 - Figure 8-A).

1. The Command Security Manager will provide departments with sequentially numbered courier cards for use by personnel in the transporting of classified material aboard NAS Oceana. They will expire at the end of each calendar year.
2. The department will institute a courier card control procedure for controlling use of the courier cards. The cards will be issued to an individual for a particular trip and receipted back in upon completion of the trip utilizing a log similar to Figure 8-B.
3. The cards will be inventoried at 1530 each working day and any outstanding cards will be recalled. Any lost, missing or unaccounted for cards will be reported immediately to the Command Security Manager.
4. Prior to issue of a courier card, the control point will obtain the destination, estimated time of return and an inventory of material involved from the courier.

8-9 Courier Authorization Off-base NAS Oceana. Courier authorization is required for hand carrying secret or confidential material while on official business from NAS Oceana provided the following conditions are satisfied:

1. The Commanding Officer or the Command Security Manager determines that the material must be hand carried.
2. A determination is made that the material is not available at the activity being visited.
3. The material cannot be transmitted by normal channels in advance of the visit.
4. The material is properly packaged and not opened, read or displayed or used in any manner while en route.
5. A list of all material being carried shall be maintained by the Command Security Manager.
6. An Authorization to Transport Classified Material will be obtained from the Command Security Manager (see Figure 8-C).

8-10 Hand Carrying Classified Documents/Packages Aboard Commercial Aircraft. Persons required to carry classified documents/packages for official duties aboard commercial aircraft must be authorized to carry classified material by the Commanding Officer or the Command Security Manager.

1. The Command Security Manager will prepare a letter of authorization upon receiving a memorandum from the cognizant department for which material is being handled (Figure 8-D).
2. The Command Security Manager will brief the authorized courier on the documentation, process and boarding procedures required. Instructions for hand carrying classified material are outlined in reference (a), Chapter 16.
3. The Command Security manager shall maintain a list of all classified material carried or escorted by traveling personnel. Upon return, all classified material must be accounted for.

CHAPTER IX
DESTRUCTION

20 JUL 1987

9-1 Policy. All classified material is accountable and, when no longer required, will be destroyed in accordance with OPNAVINST 5510.1 (series), Chapter 17. Completed destruction will be promptly reported to the Admin Support Services Supervisor in order to keep an accurate base inventory.

9-2 Method of Destruction

1. Classified material shall be destroyed either by disintegrating material or by complete burning of the material during scheduled times. Microfilm shall not be processed in shredding machines.

2. Magnetic tapes, disc packs, drums and other similar magnetic storage devices may be declassified as follows:

a. All storage locations will be overwritten a minimum of three times, once with a binary digit "1", once with the binary digit "0" and once with a single numeric, alphabetic or special character. Such alphanumeric or other unclassified data will be left on the device.

b. If the storage device has failed in such a manner that it cannot be overwritten, the device may be declassified by exposing the recording surface(s) to a permanent magnet having a field strength at the recording surface of at least 1,500 OERSTEDS.

9-3 Responsibilities and Destruction Records

1. The Command Security Manager is responsible for ensuring that proper destruction of all classified material is carried out. When classified material is placed in a burn bag for disposal the record of destruction will be signed by the witnessing official(s) at the time the material is placed in the burn bag. The individual at the command designated as the witnessing official shall be determined as follows:

- a. Top Secret - Top Secret Control Officer
- b. Secret - Departmental Custodian of Material
- c. Confidential - Departmental Custodian of Material
- d. CMS Material - CMS Custodian
- e. NWP Material - NWPL Custodian

2. Top secret or secret material to be destroyed will be recorded on the Record of Destruction (OPNAV Form 5511/12 - Figure 9-A) and confidential material on the Classified Material Inventory (NAS Oceana Form 5511/1 - Figure 5-C) then placed in the burn bag. One of the officials for top secret material must be the Top Secret Control Officer. At least one of the officials for any material must be an E-5/GS-5 or above with proper clearance.

a. The custodian preparing the destruction report will prepare for destruction by placing all material for destruction in sequential order by year and MCF control number in order to type a smooth destruction report. Thorough identification of the material being destroyed, including copy numbers, numbers of enclosures, etc., will be recorded on the smooth destruction report. When the smooth has been prepared the two witnessing officials will perform the following:

(1) Identify each document being destroyed ensuring it is described on the Destruction Report adequately and that the description agrees with the MCF.

(2) The two witnessing officials will sign and date the destruction report after all material has been sighted, inventoried and placed in the burn bag for destruction.

b. The following shall be entered on the destruction report:

- (1) Classification of destruction report.
- (2) Identification of material originator.
- (3) Serial number of material.
- (4) Date of material.
- (5) Copy number.
- (6) MCF control number.
- (7) Number of each enclosure.
- (8) Total number of pages.
- (9) Specify "RESIDUE" or "ACTUAL CHANGE" when changes are being destroyed.
- (10) Signature of individual authorizing destruction.
- (11) Date of destruction.
- (12) Signature of witnessing official(s).
- (13) Page number of destruction report.
- (14) Total number of bags destroyed (record burn bag numbers on destruction report).

c. Destruction of confidential material may be recorded on a Classified Material Inventory (NAS Oceana Form 5511/2 - Figure 9-B) and the original MCF.

d. All destruction forms will be retained for two years.

9-4 Burn Bags. Heavy RED STRIPED burn bags are to be used for classified waste and are available from SERVMART. Waste containers for disposal of classified trash are to be marked and located away from regular waste receptacles.

1. Custodians will write the highest classification of material contained in a burn bag, the date, the department code and a serial number on the burn bag. All burn bags will be assigned a serial number. The total number of burn bags will be entered at the end of the destruction report, including the serial numbers (total number of bags 3 - # 33, 34, 35).

a. No unclassified documents shall be placed in burn bags, except message traffic and material subject to the Privacy Act of 1974.

b. Bags shall not exceed ten pounds in weight.

c. Burn bags will be adequately sealed by stapling them shut at the top.

2. Each burn bag will be protected by the measures required for the highest level of classification they contain. Burn bags ready for destruction are to be stored in one location and safeguarded accordingly. Burn bags will be secured in a locked security container when an office is vacated for any reason.

3. Destruction shall be witnessed by two persons, one of which must be at the E-5/GS-5 level or above, who are cleared to the level of material being destroyed. Before destruction, burn bags should be recounted and serial numbers checked to ensure all are accounted for and burn records are accurate.

20 JUL 1987

9-5 Destruction Equipment**1. Shredders**

a. Many departments have shredders, however, the shredders vary in their degree of effectiveness depending on the mechanical condition of the equipment and the supportive security procedures that are followed.

b. The ability to process paper in shredders is limited to a maximum of two to five sheets at a time (depending on the type of paper), two automatic data processing (ADP) cards inserted side by side, double sheets of carbon paper and other similar light loads.

2. Disintegrator

a. Destruction of classified information by use of the base dry mulch disintegrator is an approved method of destroying manuals, (broken down) unseparated computer printouts, carbons, ADP cards, blueprints and all paper products. Plastics and typewriter ribbons cannot be done.

b. The disintegrator is located in building 232, Base Communications, and is available to all departments and tenant activities from 0800 to 1600 seven days a week. The disintegrator must be operated by at least one properly trained person, designated in writing by the department head or a command official and qualified by base communications.

c. To schedule an opportunity for destruction, contact the base communications watch supervisor at 433-3386/3387. Appointments are limited to two hours.

d. Due to the hazardous noise level of the disintegrator, personnel operating or in close vicinity of the disintegrator when it is in use shall use sound attenuators. Sound attenuators are available at base communications.

9-6 Emergency Destruction. The Commanding Officer will direct the emergency destruction of classified material if the requirement exists. This requirement will be met by destroying material on a priority basis; therefore, the highest priority material will be indicated in the container inventory. See Chapter XIII for the Emergency Action Plan.

20 JUL 1987

CHAPTER X

CLASSIFICATION/MARKING

10-1 Policy. Unnecessary classification and higher than necessary classification shall be scrupulously avoided. When doubt exists as to which of two designations of security classification is applicable, the higher designation should be used. The use and application of security classification shall be limited to only that which is essential to national security. The Admin Support Services Supervisor and the Command Security Manager are available for assistance in marking if required.

10-2 Classification Designations. Official information or material which requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three categories, namely, "Top Secret", "Secret" or "Confidential", depending upon the degree of its significance to national security. The markings "For Official Use Only" and "Limited Official Use" are not to be used to identify classified information (see Figure 10-A).

10-3 For Official Use Only. This term is not a security classification; therefore, it is not monitored through the Command Security Manager. However, in order to avoid improper marking, the following is germane:

1. The term FOR OFFICIAL USE ONLY and the abbreviation "FOUO" may be applied to information which may warrant protection or controlled distribution in the public interest.
2. The term FOR OFFICIAL USE ONLY shall be removed promptly when there is no longer a specific justification for protecting such information. The originator or higher authority shall be responsible for determining the date when this term shall be removed and for so notifying all addresses concerned. SECNAVINST 5570.2 series applies.

10-4 Original/Derivative Classification

1. Original Classification. The initial determination of the degree of classification to be assigned to official information. Commanding Officer, NAS Oceana is not designated as an original classification authority.

2. Derivative Classification. The application of classification markings to information which is already classified. Persons who apply derivative classification shall take care to determine whether their paraphrasing, restating or summarizing of classified information has removed all or part of the basis for classification. Assistance in classification decisions may be obtained from the Command Security Manager. Persons who apply such derivative classification markings shall:

- a. Respect original classification decisions.
- b. Verify the current level of classification of the information before applying the markings.
- c. Carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings.

(1) A classification guide, based upon classification determinations made by original classification authorities, is promulgated for each system, plan, program or project involving classified information. CNO (OP-009D) promulgates all Department of the Navy classification guides, separated into major subject categories under the OPNAVINST 5513 series (see Figure 10-B). Classification markings included the downgrading, declassification and regrading caveats must be determined from the classified information utilized or from the classification guides on a project. Any questions regarding the classifications must be referred to the originators of the original information. Questions that cannot be satisfactorily resolved must be referred to CNO (OP-009D). If there is a doubt concerning a classification marking to be applied, and it cannot be resolved, a tentative classification must be applied to the material by NAS Oceana until further guidance is received.

10-5 Downgrading and Declassification. The original classifying authority holds the responsibility for the downgrading, declassification and regrading of all material classified by them. The classification guides available in OPNAV 5513 and Exhibit 10-B will indicate what the appropriate downgrading, declassification and reclassification action will be. In other instances, this information must be extracted from the material from which the classification is determined. It is important to observe the requirements for accomplishing downgrading and declassification actions as expeditiously as possible. Declassification and downgrading shall be given the emphasis comparable to that accorded classification. The Command Security Manager shall be responsible for the review and remarking of that material authorized for downgrading and/or declassification.

10-6 Tempest. Any electrical/electronic equipment which prepares, handles, transmits, or stores classified information including word processing must have a TEMPEST survey performed. Classified material should be typed and processed by Station Admin. The survey is performed by Naval Electronic Systems Engineering Command (NAVELEX). Any department which acquires new equipment or moves existing equipment will forward a memorandum to the Security Manager, with a copy to the ADP Security Officer informing him of the need for a TEMPEST request. Departments will keep the Security Manager informed of any changes in equipment, location, or building modification. The Security Manager will request TEMPEST surveys for the command, maintain backup files for four years, and forward modifications on the original requests if necessary.

10-7 Classification Markings. The basic purpose for applying markings to documents or material containing or revealing classified information is to communicate to a recipient the degree of protection required and to facilitate extracting, paraphrasing, upgrading, downgrading and declassification actions. It is imperative that all Department of the Navy commands utilize standard markings--otherwise this basic purpose will not be realized.

1. At the time of origin, paper copies of derivatively classified documents shall show on their face:

a. The source of classification, i.e., a source document or classification guide. If classification is derived from more than one source, the phrase "multiple sources" shall be shown and the identification of each source shall be maintained with the file or record copy of the document. (See Figure 10-A for multiple sources sample.)

b. The office of origin of the derivatively classified document:

(1) Both Paragraphs a and b above refer to the "classified by" line.

c. The overall classification of the document.

d. The date or event for declassification or for review for declassification, carried forward from the classification source. If the classification is derived from multiple sources, the latest date or event shall be shown.

e. Any downgrading action to be taken and the date thereof.

2. Documents shall be marked on the front cover, title page, back cover (outside) and each interior page with the highest overall classification of the material enclosed. The classification markings should be at the top and bottom of the center of the page. (See Figure 10-C.)

3. On correspondence, such as letters and memoranda, the overall classification should be typed at the upper left, and stamped and typed at the upper and lower center of each page.

4. It is emphasized that classification markings of TOP SECRET, SECRET, and CONFIDENTIAL shall be stamped, printed or written in capital letters (not typing alone) that are larger than those used in the text of the document and, when practicable, red in color.

5. All reproductions or copies of classified materials, regardless of form, shall bear clearly legible security markings and notations in the same manner as on the original material from which copied or reproduced. In this connection, it should be noted that office-type copying equipment does not always clearly reproduce all colors of ink or marginal images. Therefore, if the reproduction process employed does not faithfully reproduce the security markings appearing on the original copies such markings shall be stamped on all copies in the same positions and size required for the original.

10-8 Use of Cover Sheet. Classified material in routing or handled in an office environment, is in constant danger of becoming intermixed with unclassified documents, inadvertently placed in unclassified trash, viewed by uncleared personnel, or otherwise mishandled due to failure of the individuals concerned to recognize it as classified. Accordingly, all classified material shall be covered by the appropriate Standard Form 703, 704, or 705 cover sheet.

20 JUL 1987

10-9 Marking Components. Major components of documents or correspondence may be utilized separately; therefore, these components should be classified as a separate document. Examples include, enclosures, annexes, appendices or attachments.

10-10 File or Folder Marking. Files, folders or groups of documents shall be conspicuously marked top, bottom, front and back to assure their protection to a degree as high as that of the most highly classified document therein. "Classified Material Attached" warning attachments (OPNAV Form 5216/96 (Rev. 11-76)) may be utilized for this purpose.

10-11 Portion and Paragraph Marking

1. (TS), (S), (C) and (U) will precede each portion, section, paragraph or subparagraph of a classified document. Each part will be marked for its content alone. Subordinate parts need not be marked if the classification is the same as the lead-in portion (Figure 10-C).

2. The classification markings shall be displayed after each subject, heading or title. The markings will indicate only the classification of the heading or title itself, and not the overall classification of the material that follows.

10-12 Warning Notices. When applicable, one or more warning notices shall also be prominently displayed on classified documents or correspondence. These notices should be conspicuously marked only once on the cover or first page of the material. Warning notices shall be printed verbatim as found in Figure 10-A of this instruction.

10-13 Electrically Transmitted Messages. A sample classified message is included in Figure 10-D.

10-14 Marking of Card Decks. Card decks shall be classified when classified information is contained therein or may be derived from them by use of the deck. The overall classification assigned shall be at least as high a level as the highest classification of any information revealed by the use of the card deck. A deck of classified accounting machine cards need not be marked individually, but may be marked as one single classified document so long as all cards remain within the deck.

10-15 Automatic Data Processing (ADP) Tapes and Word Processing Storage Media

1. Information storage media and devices, used with Automatic Data Processing (ADP) systems and typewriters or word processing systems, must be marked externally to clearly indicate the classification of the information they contain and the associated marking.

2. ADP systems and word processing systems will provide for internal markings to ensure that classified information which is reproduced or generated clearly shows the classification and associated markings. Chief of Naval Operations (OP-009P) may exempt existing systems when internal marking requirements cannot be met without extensive system modification. Procedures must be established, however, to ensure that users and recipients of the media or the information are clearly advised as to the classification and associated markings.

10-16 Conclusion

1. Classification/markings/downgrading/declassification are all critical parts of a complicated and exacting security protection process. Assistance is available from the Admin Support Services Supervisor and Command Security Manager. It is a most important function in the protection of classified material. It is important in making sure persons know what needs protection and how it should be protected and is the primary means of passing on necessary data about classified information to those who "need to know".

2. Exhibits 9A through 9I in OPNAV 5510.1 (series) are helpful as a reference when marking classified material.

CHAPTER XI
CONTROL OF VISITORS

11-1 Incoming Visits

1. The Command Security Manager with the administrative assistance of the Assistant Security Manager shall exercise security control over classified visits to and from this command and is the central control point for receiving and recording incoming visit requests from DOD and contractor activities.

a. Upon receipt of an incoming visit request, the Command Security Manager will forward a copy to the point of contact and retain master files. If offices to be visited receive a visit request directly, the request must be forwarded to the Command Security Manager for recording purposes.

b. Visit requests received by mail or message in which the cognizant department/division is not readily identifiable or for which the purpose is vague will be carefully reviewed by the Command Security Manager. Telephone inquiry will normally determine appropriate cognizance for routing purposes. When cognizance cannot be determined, the Command Security Manager will obtain clarification from the requesting activity.

c. The Command Security Manager will determine in each case involving access to classified information (classified visit requests) whether the visit request and related data are correct and thus acceptable. The responsibility for denial or removal of a visitor, however, is not delegated and shall be retained by the Commanding Officer.

d. The Command Security Manager will review all directives (in rough draft or by copy to) promulgated concerning visits to determine any special precautions that should be promulgated/established to offset possible unauthorized disclosures or compromise of classified information.

2. The Base Security Officer shall:

a. Provide base in-transit escort and security for VIP's when required.

b. Require proper identification of visitors entering the air station.

3. Department/divisions receiving visit requests for which action or cognizance is improperly indicated shall act promptly to have action reassigned when the cognizant office is known by notifying the Command Security Manager. Department heads shall:

a. Ensure that access to classified material during a classified visit is based on need-to-know, and only then after identification and security clearance has been verified.

b. Provide escorts to/for visitors that do not have clearance, or who are not visiting the command on a "classified visit," based on a classified visit request. The movement of all visitors shall be restricted as may be necessary to protect classified information. As a matter of convenience and courtesy, flag officers, general officers and their civilian equivalents shall not be required to sign visitor records or display identification badges when being escorted as visitors. This will be done by the escort, if required, as identification of these senior visitors by escorting personnel should normally be sufficient. Care should be exercised to ensure that escorting personnel are present at all times to avoid challenge or embarrassment and to ensure that necessary security controls are met. Whenever an escort is not provided or not present, the visitor must comply with all normal security procedures. When escorts are utilized, they are responsible to the Commanding Officer to ensure that the visitor has access only to that information which he/she has been authorized to receive.

c. Ensure that a departmental visitor's control log is maintained for restricted areas. All entries by foreign nationals must be logged. Entries by U.S. citizen visitors or staff personnel must be logged when entry occurs after normal working hours.

11-2 Outgoing Visits. Requests for visits by NAS Oceana personnel, which will necessitate their having access to classified information, will normally be made by using the Visit Request Form (Visitor Clearance Data) OPNAV Form 5521/27. It should be filled in by the initiating office and forwarded to the Command Security Manager for security certification.

Requests for visits shall be submitted in advance of the proposed visit and in sufficient time to permit processing. In exceptional cases, the above information may be furnished by telephone or other means or rapid communication, provided such information is confirmed promptly in writing. When a telephone request is made, the visit request shall be submitted to the Command Security Manager prior to arranging the oral visit request. NAS Oceana departments making arrangements for sponsored visits that include personnel from other DOD or contractor agencies should notify those activities to forward security confirmation for their personnel to the activity to be visited. When submitting a visit request to a DOD activity, the Command Security Manager requires a typed envelope addressed to that activity along with the visit request. Under no circumstances may personnel hand carry their own visit request to the place being visited. Figure 11-A provides a guide for preparation of a visit request in message form. Messages will only be utilized when there is less than five days lead time between scheduling and commencement of visit.

11-3 Visit to Contractor Facilities. When personnel require access to classified information in connection with a visit to a contractor facility, the visit request shall be submitted as in paragraph 11-2, with one exception - an information copy shall be submitted to the appropriate Defense Investigative Service Cognizant Security Office. The NAS Oceana department submitting a visit request to a contractor facility will forward to the Command Security Manager a visit request, an addressed envelope to the activity and an addressed envelope to appropriate DIS Cognizant Security Office. Under no circumstances are departments to make prior notification or oral request for visits.

11-4 Visits by Representatives of the General Accounting Office. Properly cleared and identified representatives of the General Accounting Office (GAO) may be granted access to classified Department of the Navy information in the performance of their assigned duties and responsibilities in accordance with paragraph 18-8 of OPNAVINST 5510.1. All GAO visit requests will be kept on file in the Command Security Manager.

11-5 Visits by Contractors

1. All visit clearance requests for contractors, in connection with NAS Oceana contracts, must be forwarded to the Command Security Manager.
2. After approval, the Command Security Manager will enter the contractor's name, clearance, date of request and date of visit expiration in the listing of personnel authorized to visit. A maximum of twelve (12) months visit or expiration of contract, whichever is shorter, is accepted by NAS Oceana.
3. Contract personnel must submit requests for copies of classified material to their contracting officer. NAS Oceana personnel will not supply copies of classified material to contract personnel. It is the contracting officer's responsibility to ascertain the contractor's need for the material and that proper storage can be afforded the material. The contracting officer will request the desired material for the contractor officially from the command. The material will be forwarded by the classified control point which has cognizance over the material to the contracting officer, who will transfer custody of the material to the contractor.

11-6 Expiration of Visit Requests. Visit requests may be submitted for a period up to one year. When an employee resigns, retires or transfers, NAS Oceana departments will notify the Command Security Manager so that action may be taken to cancel the individual's visit request at other installations.

11-7 Visit Reports. The Command Security Manager shall be immediately informed when any visitor expresses an unusual interest in information that he is not authorized to receive or expresses feelings inimical to the best interest of the United States.

11-8 Meetings. Protection of classified information within a conference room is the responsibility of the office sponsoring the conference. The sponsoring office will coordinate arrangements with the Command Security Manager. The office conducting the conference, briefing or presentation will cause an inspection to be made at the conclusion thereof to

20 JUL 1987

ensure that no classified information remains in the room. All offices conducting meetings should be familiar with the guidelines of Chapter 19 of OPNAVINST 5510.1 (series).

1. For conferences or meetings in which classified material is to be discussed, the officer scheduling the conference is responsible for providing a monitor for the passageway adjacent to the conference room while the conference/meeting is in session. Such monitors must have a security access equivalent to the classification of the conference. The Security Manager can assist in coordinating arrangements and instructions for monitors.

2. If any telephones are located in the conference rooms, the sponsoring office shall arrange for their disconnection during classified discussions.

CHAPTER XII

EMERGENCY PLAN FOR THE PROTECTION
OF CLASSIFIED MATERIAL

12-1 General

1. The emergency plan for the protection of classified material shall be implemented whenever Naval Air Station Oceana is threatened with any of the following:

- a. Natural disaster - flood; hurricane; tornado.
- b. Casualty - fire; accidental explosions.
- c. Occupational - enemy attack; riot.
- d. Destruction by any means.
- e. Abandonment by own forces due to any cause.

2. Since emergencies of a natural or casualty nature would not normally subject classified material to capture by enemy forces, securing or removing the material, as directed, should suffice. In the case of fire, however, the primary consideration is the safety and welfare of personnel. If it is not possible to safely secure or remove classified material, it will be left in place to be consumed by the fire. **UNDER NO CIRCUMSTANCES WILL ANYONE SUBJECT HIMSELF OR HIS SUBORDINATES TO DEATH OR INJURY TO PROTECT CLASSIFIED MATERIAL FROM FIRE.**

3. In the event CMS material is destroyed by accidental fire, the Command Duty Officer will procure the identification of all firefighting personnel entering the spaces. Additionally, the CMS Custodian and Local Holder Custodians, if applicable, will be the first persons to enter the spaces when the fire has been extinguished and safety permits. At this time they will ensure that all CMS distributed materials have been totally destroyed or provide adequate storage for those items not completely destroyed.

4. When hostile action occurs, it must be assumed that classified material is a target and all actions must be directed at keeping the material from unauthorized personnel by protecting, relocating or destroying the material as conditions dictate.

12-2 Implementation. Under normal circumstances the Commanding Officer, NAS Oceana will order the emergency protection plan implemented when it is considered that the forces and facilities at his disposal are inadequate to protect classified material from impending loss or capture. Should conditions prevent contact with the Commanding Officer, the senior officer present is authorized to initiate the plan without awaiting specific orders. Exercising individual initiative in preparing for emergency action at all levels of command is desired. The senior officer present shall recognize that he is senior and shall accept the responsibility to act.

12-3 Procedures. All procedures affecting Communications Security Material (CMS) shall be pursuant to NASOCEANAINST 5510.1.

1. Protecting. When ordered to secure classified material, all hands will ensure that classified documents are placed in safes and/or lockable file cabinets immediately. (Under ideal conditions, all CMS material will be returned to the CMS Custodian for stowage. The entrances to those spaces with CMS equipment installed will be secured under armed guard until the emergency is terminated.)

2. Emergency relocation will be accomplished under the following conditions:

- a. Casualty (See 12-1 above).
- b. Natural disaster.
- c. Destruction, capture or compromise by local dissidents.

d. Relocation will not be undertaken if

(1) Risk of loss of life or serious injury is great.

(2) Relocation sites are also in jeopardy.

(3) The material being relocated is not CMS, top secret or secret. (NOTE: If sufficient time and personnel are available, ALL classified material should be relocated; however, since the situation would be an emergency, and the remaining classified material would be in large quantities, removal of any confidential material will not be undertaken until all CMS, top secret and secret material is relocated and protection of that material is adequate and constant.)

3. Emergency relocation sites (on board)

a. CMS material: CMS vault, Base Communications, building 232. Alternate site: AIMD vault, building 513, room 29, workcenter 64B/C/D Avionics. (When directed to relocate CMS material to a more secure area, all Communications Division personnel in a duty status will immediately report to the CMS Custodian at the CMS vault. If sufficient numbers of personnel are not available from Communications, the Command Duty Officer will be so advised and requested to make additional personnel available immediately. Regardless of the destination for the material to be removed, the CMS Custodian will inventory, by short title, quantity and register number, all items removed from the CMS vault. The Commanding Officer will be periodically advised of the progress of the operation.)

b. Top Secret and Secret Material: Vault, Base Communications, building 232.
Alternate and/or overflow sites: AIMD vault, building 513, room 29.

c. Priority of material to be relocated

(1) CMS top secret material.

(2) Top secret material.

(3) CMS secret material.

(4) Secret material.

(5) All other CMS material.

(6) All other classified material.

d. Priority of material to be protected during relocation and after relocation

(1) CMS top secret.

(2) Top secret material.

(3) CMS secret.

(4) Secret material.

(5) All other CMS material.

(6) All other classified material.

4. Emergency Relocation (off-base). (Off-base relocation shall not be attempted if the main and/or back gates and/or roads leading to/from NAS Oceana are impassable or under control of the enemy or local dissidents. If any of these situations exist, on base relocation to the above emergency relocation sites or alternate sites will be accomplished and readiness for possible emergency destruction commenced.)

20 JUL 1987

(j) The NWPL Custodian (alternate - Communications Watch Supervisor). All classified material and equipment under his cognizance. He will be assisted by personnel from the Communications Division.

(k) Other Department Heads/Special Assistants. All classified material and equipment under their cognizance.

b. Listing of Classified Material to be Destroyed

(1) Officers assigned primary responsibility for destruction in above sub-paragraphs shall prepare lists of classified material under their cognizance. These lists shall contain the following information and be readily accessible to the person responsible for emergency destruction:

- (a) Location of classified material.
- (b) Personnel responsible for emergency destruction.
- (c) Recommended place and method of destruction.
- (d) Means of access to containers.

(2) When actual destruction is ordered, or a destruction drill is held, officers assigned primary responsibility will advise the Command Security Manager when their portion of the destruction has been completed/simulated. The Command Security Manager will report to the Commanding Officer when destruction has been reported completed/simulated by all responsible officers.

c. Methods of Destruction

(1) CMS Material - in accordance with NASOCEANAINST 5510.1, CMS Emergency Action Plan.

(2) Burnable matter by burning, followed by complete obliteration of residue by reduction to sludge or to an equivalent state. Dousing the material with a flammable liquid may prove useful when time is critical. Burning can be accomplished in drums or barrels in parking lots in bonfires. NOTE: In an emergency, gasoline can be drained from the private automobiles (not emergency vehicles) to enhance burning.

(3) The disintegrator in Base Communications, building 232, will be used for the destruction of the most sensitive material (CMS, top secret) first. After the destruction of this material, other material may be destroyed in the disintegrator with no regard for the waste material emptying into the dumpster.

(4) Classified equipment by damaging beyond recognition or reconstruction through use of sledge hammers, cutting tools or torches.

(5) If destruction cannot be completed prior to eminent capture, material should be scattered, mixed with refuse in dumpsters and ignited, jettisoned in weighted containers in lakes, flushed into drains or disposed of using any method to destroy or obliterate to every degree possible.

d. Priority of Emergency Destruction

(1) Classified material shall, when practicable, be color coded to indicate its priority for emergency destruction. In general, emergency destruction of classified material should be accomplished pursuant to the following priorities:

- First: Blue - COMSEC material marked "TOP SECRET"
- Second: Red - "TOP SECRET" material
- Third: White - COMSEC material marked "TOP SECRET"
- Fourth: Yellow - Secret material

a. The Commanding Officer, Executive Officer, CDO, OOD or senior officer present, or if those officers have been incapacitated, shall request relocation site assistance from:

- (1) COMFITMATAEWINGSLANT Duty Officer
- (2) COMNAVAIRLANT Duty Officer, 444-2928
- (3) COMNAVBASE, Norfolk Duty Officer, 444-7097

b. If none of the commands are able to provide relocation site assistance, any command that is not affected by the situation shall be contacted. (It is reemphasized that relocation or destruction too early or unnecessarily is better than to have taken no action at all).

5. Emergency Destruction

a. Responsibility for Emergency Destructions

(1) The Commanding Officer (or successively in his absence, the Executive Officer, CDO or OOD) will implement the emergency destruction of classified material. However, should circumstances warrant, the senior individual present in a space containing classified material may initiate emergency destruction of classified material.

(2) The importance of beginning destruction sufficiently early to preclude loss of classified material to the enemy cannot be overemphasized, as the effects of premature destruction are considered relatively inconsequential when measured against the possibility of compromise.

(3) The following are assigned primary responsibility for destruction of classified material indicated:

(a) The CMS Custodian (alternate - Alternate CMS Custodian). All CMS distributed publications, classified communication material and equipment under his cognizance.

(b) The Top Secret Control Officer (alternate - Assistant Top Secret Control Officer). All top secret material under his cognizance.

(c) The Administrative Officer (alternate - Assistant Administrative Officer). All classified material and files located in offices in the Administrative offices. He will be assisted by personnel from the Support Services Office and Admin Division.

(d) The Air Operations Officer (alternate - Assistant Air Operations Officer). All classified material and equipment under his cognizance. He will be assisted by personnel from the Air Operations Department.

(e) The Weapons Officer (alternate - Leading Chief Petty Officer). All classified material and equipment under his cognizance. He will be assisted by personnel of the Weapons Department.

(f) The AIMD Officer (alternate - Assistant AIMD Officer). All classified material and equipment under his cognizance. He will be assisted by personnel of the AIMD department.

(g) The Supply Officer (alternate - Assistant Supply Officer). All classified material and equipment under his cognizance, including classified material in a warehouse awaiting deliver/shipment. He will be assisted by personnel from the Supply Department.

(h) The Public Works Officer (alternate - Assistant Public Works Officer). All classified material and equipment under his cognizance. He will be assisted by personnel from the Public Works Department.

(i) The Civilian Personnel Officer (alternate - Assistant Civilian Personnel Officer). All classified material and equipment under his cognizance. He will be assisted by personnel from the Civilian Personnel Department staff.

20 JUL 1987

Fifth: Green - Confidential material

Sixth: Unclassified - equipment which would be of use to an enemy, together with pertinent technical, descriptive and operating instructions.

e. Department heads/special assistants having responsibilities for classified material shall develop written plans and procedures to implement their responsibilities, including necessary supporting data, recall bills, general emergency bills, fire bills, etc. A copy of these plans shall be furnished to the Command Security Manager for inclusion as appendixes to this chapter.

f. The Command Security Manager is responsible for this bill and testing its effectiveness at least annually.

20 JUL 1987

MARKING GUIDE FOR PUBLICATIONS AND CORRESPONDENCE
(Refer to OPNAVINST 5510.1 series for marking
requirements for other types of material.)

Table 1

*Required Marking

MARKING	PLACEMENT
<p>*Classification - TOP SECRET, SECRET OR CONFIDENTIAL</p>	<p>On Publications, stamped or printed TOP and BOTTOM center in letters larger than other print, preferably in red, on the front cover (if any), on the title page (if any), on the first page and on the outside of the back cover (if any). If the back cover is not used, classified text may not appear on the back of the last page. Mark interior pages of publications either with the overall classification or with the classification of the individual page. When exercising the individual page option in cases of front and back printing both sides of the page must be marked with the highest classification of either side. The side with the lower classification should be indicated at the bottom with the statement "This page is Unclassified" or other classification as appropriate.</p> <p>On the first page of correspondence, typed at the upper left in addition to the markings described above.</p>
<p>CLASSIFIED BY (Insert) Insert the identity of the original classification authority or derivative classification source. (OPNAVINST 5510.1G lists original classification guides or other classified documents are derivative sources.) If more than one source is used, insert the phrase "Multiple Sources" and list all sources on the official record copy.</p>	<p>Once at lower left of the covering (first) page.</p>
<p>DECLASSIFY ON (Insert date or event or "OADR"). Insert the declassification date or event. If neither of these can be predetermined, insert the notation "Originating Agency's Determination Required" or its abbreviation "OADR".</p>	<p>Once at lower left on the covering (first) page beneath the "CLASSIFIED BY" line.</p>

FIGURE 10-A

20 JUL 1987

<p>DOWNGRADE TO (insert classification level) ON (insert date or event)</p>	<p>Once at lower left on the covering (first) page above the "DECLASSIFY ON" line.</p>
<p>(UNCLASSIFIED), (SECRET) or (CONFIDENTIAL) UPON REMOVAL OF ENCLOSURE (or specific enclosure, as applicable) This marking is required on letters or documents of transmittal which cover enclosures of a higher classification.</p>	<p>Top left following classification marking (the classification marking must equal the highest classification of any enclosure being transmitted). Mark second and succeeding pages at TOP and BOTTOM center with the classification of the transmittal letter or document itself; if it is unclassified, no marking is required.</p>
<p>*AGENCY AND OFFICE OF ORIGIN (required if not otherwise evident). DATE OF ORIGIN</p>	<p>Once on the covering (first) page.</p>
<p>*(U), (C), (S), (TS) (required for all paragraphs, subparagraphs, titles, headings, captions, etc). Naval nuclear propulsion information (NNPI) will not be portion marked.</p>	<p>Once on the covering (first) page. Before each paragraph or portion (except NNPI) and before each caption. After headings and titles. (Use unclassified titles whenever possible to facilitate indexing).</p>
<p>CLASSIFIED BY DEO-DOD classification guide CG-RN-1 dated January 1977. DECLASSIFY ON: Originating Agency's Determination Required. This document shall not be used as a derivative classification source (required marking for NNPI).</p>	<p>Once on covering (first) page.</p>
<p>WARNING NOTICES</p>	<p></p>
<p>RESTRICTED DATA This material contains Restricted Data as defined in the Atomic Energy Act 1954. Unauthorized disclosure subject to administrative and criminal sanctions (full notice) RESTRICTED DATA (short form), RD (abbreviated form).</p>	<p>RESTRICTED DATA Full notice at lower left on the covering (first page) beneath the "CLASSIFIED BY" line, in lieu of a "DECLASSIFY ON" line. Short form typed after classification at the top left on the first page of correspondence. Abbreviated form following portion marking classification symbol, e.g., (S-RD or S-FRD)</p>
<p>FORMERLY RESTRICTED DATA Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restrictive Data in foreign dissemination. Section 144b Atomic Energy Act of 1954 (full notice), FORMERLY RESTRICTED DATA (short form), FRD (abbreviated form)</p>	<p></p>

FIGURE 10-A

TO:

FROM (Name and address of activity)

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

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

DESCRIPTION OF MATERIAL

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

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

DATE OF DESTRUCTION

WITNESSING OFFICIAL (Signature, Rank/Rate/Grade)

WITNESSING OFFICIAL (Signature, Rank/Rate/Grade)