DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

SPAWARINST 5510.3H
SPAWAR 10H
20 December 1988

SPAWAR INSTRUCTION 5510.3H

From: Commander, Space and Naval Warfare Systems Command

Subj: SPACE AND NAVAL WARFARE SYSTEMS COMMAND SECURITY MANUAL

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5530.14A
(c) OPNAVINST 3070.1A

1. Purpose. To update security policy and procedural guidance for the protection of classified information, government property and personnel within or under the custody of or under the cognizance of the Space and Naval Warfare Systems Command.

2. Cancellation. SPAWAR Instructions 5510.3G and 5239.2 are hereby cancelled and superseded.

3. Scope. This instruction covers all Space and Naval Warfare Systems Command security policies and procedures developed in implementation of the Command security program. It is issued in accordance with the provisions of references (a), (b) and (c).

4. Action. All personnel shall fully comply with the provisions of this instruction. SPAWAR activities shall comply to the extent outlined by Chapters VI, VII, VIII and IX.

John C. Weaver
JOHN C. WEAVER
Rear Admiral, U.S. Navy

DISTRIBUTION:
SPAWAR List 7

SNDL Part II:
FKQ (SPAWAR Activities - 5 copies)

Copy to:
SNDL Part II:
A4A

Stocked:
SPAWAR 10H (1500 copies)

RECORD OF CHANGES

Identification of Correction or Change	Date Entered	By whom entered (signature, title, command)

TABLE OF CONTENTS

		Page Number
CHAPTER I - INTRODUCTION		
0101	Purpose	1-1
0102	Security Principle	1-1
0103	Command Responsibility and Authority	1-1
CHAPTER II - HEADQUARTERS/BUILDING SECURITY		
SECTION 1 - Control of Classified Material		
0201	General	2-1
0202	Access to Classified Material	2-1
0203	SPAWAR Central Classified Material Custodian	2-1
0204	Accountability and Control	2-1
0205	Classified Material Control Record (Route Sheets)	2-5
0206	Retaining or Copying Classified Documents	2-5
0207	Handling Precautions and Office Practice	2-6
0208	Control of Classified Working Papers or Preliminary Drafts	2-7
0209	Distribution Lists for Classified Documents	2-8
SECTION 2 - Transmission		
0210	General	2-9
0211	Hand-carrying Classified Information on Commercial Aircraft Within CONUS	2-10
0212	Hand-carrying Classified Material Outside CONUS	2-13
0213	Travel of Personnel Having Knowledge of Sensitive Information and Personnel Conduct in the Event of Hijacking	2-13
0214	Transmission and Preparation	2-14
SECTION 3 - Office Classified Material Custodian		
0215	Definition	2-19
0216	Criteria for Selection	2-19
0217	Training	2-19
0218	Responsibilities	2-20
SECTION 4 - Destruction of Classified Material		
0219	Authority	2-21
0220	Requirements and Procedures	2-21

		Page Number
SECTION 5 - Security Stowage		
0221	Security Container Custodian	2-21
0222	Combinations	2-22
0223	Stowage	2-23
0224	Stowage Equipment	2-23
0225	Locking Procedures	2-24
0226	Security During Emergencies	2-25
0227	Daily Security Inspection	2-26
0228	Care After Working Hours of Stowage Cabinets	2-27
0229	Areas Protected by Electronic Intrusion Devices	2-28
SECTION 6 - Security Coordinators		
0230	Directorate, Project Office and Staff Office Security Coordinators	2-28
SECTION 7 - Security Inspections		
0231	General	2-30
SECTION 8 - Security Training and Education		
0232	Security Education	2-31
SECTION 9 - Building Security Regulations		
0233	General	2-35
0234	Security Hours and Sign in/out procedures	2-35
0235	Admittance	2-35
0236	DoD Building Passes	2-37
0237	Property Passes	2-37
0238	Photographic, Video and Audio Recording Equipment	2-38
0239	Weapons and Explosives	2-38
SECTION 10 - Department of Defense Building Passes		
0240	Loss of Property, Thefts, and other Irregularities	2-38
0241	Responsibility	2-38
0242	Types of DoD Building Passes (Partial Listing)	2-39
0243	Loss of DoD Building Pass	2-39

		Page Number
SECTION 11 - Visits and Visitor Control		
0244	Surrender of Building Pass	2-40
0245	Visitor Categories	2-40
0246	Visits to SPAWAR	2-40
0247	Visits by SPAWAR or SPAWAR Sponsored Personnel	2-45
0248	Unauthorized Visitors	2-46
0249	Area Control	2-46
SECTION 12 - Security Violations		
0250	General	2-47
0251	Reporting Violations	2-47
0252	Investigation of Violations	2-47
0253	Disciplinary Action	2-48
SECTION 13 - Meetings, Conferences, and Symposia		
0254	General	2-49
0255	Responsibility for Classified Meetings Held at SPAWAR Headquarters	2-49
0256	Responsibility for Classified Meetings Held Outside SPAWAR Headquarters	2-50
0257	Physical Security Requirements	2-51
SECTION 14 - Non-SPAWAR Personnel Assigned to SPAWAR		
0258	Definition	2-52
0259	Identification and Authority	2-52
0260	Action	2-52
0261	Reporting Violations	2-54
SECTION 15 - Questionnaires		
0262	Discussion	2-54
0263	Policy	2-55
0264	Action	2-55
SECTION 16 - Communist Propaganda		
0265	Action	2-55
SECTION 17 - Liaison with Investigative Agencies		2-56
SECTION 18 - Unauthorized Absentees		2-56

Page Number

CHAPTER III - INDUSTRIAL SECURITY AND DOMESTIC DISCLOSURES

SECTION 1 - Industrial Security

0301	General	3-1
0302	Classified Contracts	3-1
0303	Contract Security Classification Specification (DD Form 254)	3-1
0304	Item Entries on the DD Form 254	3-2
0305	Verification of Clearances	3-2
0306	Disclosures to SPAWAR Contractors	3-3
0307	Transmittal of Classified Material to DoD Contractors	3-3

SECTION 2 - Disclosures

0308	Disclosures to Department of Defense	3-4
0309	Disclosures to Non-SPAWAR Contractors	3-4
0310	Disclosures Requiring Special Authorization	3-5

SECTION 3 - Control of Unclassified Technical Documents

0311	Applicability	3-5
0312	Definitions	3-6
0313	Policy	3-7
0314	Responsibilities	3-7

CHAPTER IV - PERSONNEL SECURITY AND SPECIAL ACCESS AUTHORIZATION

SECTION 1 - Personnel Security Clearances

0401	General	4-1
0402	Responsibilities	4-1
0403	Position Sensitivity	4-2
0404	Pre-hire Security Processing (Civilian)	4-2
0405	Procedures	4-3
0406	Upgrading Clearance	4-4
0407	Downgrading/Withdrawal of Clearances	4-4
0408	Security Indoctrination	4-4
0409	Security Agreement	4-4
0410	Termination of Clearance	4-5
0411	Factors Affecting Personnel Security Clearances	4-5
0412	Denial/Revocation of Clearance	4-11
0413	General	4-12

Page Number

SECTION 2 - Special Access Authorization

0414 Terminating Access Authorization 4-12

CHAPTER V - CLASSIFICATION MANAGEMENT

SECTION 1 - General

0501 Classification Management Program 5-1
0502 Misuse of Classification 5-1

SECTION 2 - Classification Categories

0503 General 5-1
0504 Definition of Top Secret 5-2
0505 Definition of Secret 5-2
0506 Definition of Confidential 5-2
0507 Restricted Data, Formerly Restricted Data, and CNWDI 5-2
0508 Foreign Classified Information 5-3

SECTION 3 - Authority to Classify

0509 Original Classification 5-4
0510 Derivative Classification 5-5
0511 Classification Pending 5-6

SECTION 4 - Original Classification Principles, Criteria and Considerations

0512 Judgement Requirement 5-7
0513 Identification of Specific Information 5-7
0514 Reasons for Classification 5-7
0515 Specific Classifying Criteria 5-7
0516 Classifying Research Data 5-8
0517 State-of-the-Art and Intelligence 5-8

SECTION 5 - Duration of Original Classification

0518 General 5-9
0519 Duration 5-9

		Page Number
SECTION 6 - Classification Guidance		
0520	Policy	5-9
0521	Retrieval and Analysis of Navy Classified Information (RANKIN)	5-10
SECTION 7 - Marking Requirements		
0522	General	5-11
0523	Overall and Page Marking	5-12
0524	Marking Components	5-13
0525	Portion and Paragraph Markings	5-13
0526	Compilations	5-14
0527	Subjects and Titles	5-14
0528	File, Folder, or Group of Documents	5-14
0529	Transmittal Documents	5-14
0530	Electrically Transmitted Messages	5-14
0531	Classification Markings on Special Types of Material	5-14
SECTION 8 - Downgrading, Declassification or Upgrading		
0532	Policy	5-16
0533	Converting Old Downgrading/Declassification Markings to Newly Created Information or Material	5-17
0534	Remarking Documents and Material Originated Prior to 1 August 1982	5-17
0535	Restricted Data and Formerly Restricted Data	5-17
SECTION 9 - Warning Notices		
0536	General	5-17
0537	Restricted Data and Formerly Restricted Data	5-18
0538	Dissemination and Reproduction Notice	5-18
0539	Intelligence Sources and Methods Information	5-18
0540	Naval Nuclear Propulsion Information	5-18
0541	COMSEC Material	5-19
0542	Not Releasable to Foreign Nationals (NOFORN)	5-19

Page Number

CHAPTER VI - FOREIGN DISCLOSURE

SECTION 1 - Release of Documentary Information

0601 Headquarters 6-1
0602 SPAWAR Activities 6-2

SECTION 2 - Official Visits Abroad

0603 Definition 6-4
0604 General 6-4
0605 Procedures 6-4
0606 Visits to the USSR and Bloc Countries 6-7

SECTION 3 - Local Foreign Visits

0607 Procedures 6-7

SECTION 4 - International Information Exchange Agreements

0608 Background 6-9
0609 Policy 6-10
0610 Disclosure of Classified Information 6-11
0611 Establishing and/or Participating in Exchange Agreements 6-11
0612 Responsibilities 6-11
0613 Scientist and Engineer Exchange Programs 6-12

SECTION 5 - NATO Security Procedures

0614 General 6-13
0615 Definition of Terms 6-13
0616 Security of Classified NATO Material 6-14
0617 Stowage of NATO Material 6-14
0618 Clearance 6-15
0619 Handling Procedures Within SPAWAR 6-15
0620 Application of NATO Classification 6-15
0621 U. S. Documents to be Entered into NATO 6-15

CHAPTER VII - SECURITY AT SPAWARSYSCOM FIELD ACTIVITIES

0701 Responsibility 7-1

Page Number

CHAPTER VIII - OPERATIONS SECURITY

SECTION 1 - Policy and Actions

0801	General	8-1
0802	Scope	8-1
0803	Definition	8-1
0804	Concept	8-2
0805	Policy	8-2
0806	Responsibilities	8-2
0807	Action	8-2

SECTION 2 - Operations Security Planning Criteria and Procedures

0808	Operations Security Planning Requirements	8-4
0809	Plan Development Criteria	8-5
0810	OPSEC Posture Analysis	8-7
0811	Planning Guidance	8-8
0812	Vulnerabilities	8-11
0813	Countermeasures	8-13
0814	OPSEC Plan Format and Preparation	8-17

CHAPTER IX - AUTOMATED INFORMATION SYSTEM SECURITY

SECTION I - Policies, Requirements and Guidlines

0901	General	9-1
0902	Scope	9-1
0903	Definitions	9-2
0904	Concepts and Objectives	9-2
0905	General Policy	9-2
0906	Responsibilities and Authority	9-3
0907	Specific Policy	9-6

SECTION 2 - SPAWAR AIS Security 9-10

0908	Minimum Program Requirements	9-10

SECTION 3 -

0909	Definition of Terms	9-13

EXHIBITS		Page Number
2-1	Authorization to Transport Classified Material Inside CONUS	2-A
2-2	Authorization to Carry Classified Information Aboard Commercial Passenger Aircraft	2-B
2-3	Appointment of Security Coordinator	2-C
2-4	Security Coordinator Inspection Report	2-D
2-5	Security Orientation Certificate	2-E
2-6	GSA Rules and Regulations Governing Public Buildings and Grounds	2-F
2-7	Report of Loss or Theft (GSA Form 182)	2-G
2-8	Request for DoD Building Pass for Contractor Employee	2-H
2-9	DoD Building Pass Form (Loss)	2-I
2-10	Incoming Visit Request Routing Form	2-J
2-11	Outgoing Visit Request (OPNAV Form 5521/27)	2-K
2-12	Schedule of Disciplinary Actions Form	2-L
2-13	SPAWAR MIC Physical Security Responsibilities Form	2-M
2-14	Security Agreement for Non-SPAWAR Personnel	2-N
2-15	Activity Security Checklist	2-O
2-16	Security Container Check Sheet	2-P
2-17	Request for Cardkey	2-Q
2-18	Classified Document Distribution List	2-R
3-1	Request for Proposal DD Form 254	3-A
3-2	Original Contract DD Form 254	3-B
3-3	Revised DD Form 254	3-C
3-4	Final DD Form 254	3-D
3-5	Distribution Statements for Technical Documents	3-E
3-6	Marking Instructions for Distribution Statements	3-F
3-7	Contractor-Imposed Distribution Statements	3-G
3-8	Authorization to Remove Classified Material	3-H
3-9	Review of MILSPEC/STD Handbook	3-I
4-1	Request for Security Clearance (Civilian and Military)	4-A
5-1	Example Marking Letter	5-A
6-1	Foreign Visit Authorization	6-A
6-2	Request for Approval to Visit Local Foreign Entity	6-B
8-1	Command/Staff OPSEC Plan	8-A
8-2	Format for Plans to Protect Weapon Systems Test and Performance Data for Navy Laboratories	8-B
Figure 1	Mailing of Confidential Material	2-15
Figure 2	Security Container Information and Combination Change Envelope	2-21
Figure 3	Visitor Control Guide	2-40
APPENDIX	Navy Laboratory Protection Capability Matrix	8-C
MATRIX	Activity Protection Capability Matrix	8-D

CHAPTER I

INTRODUCTION

0101. PURPOSE

The Space and Naval Warfare Systems Command (SPAWARSYSCOM) Security Manual establishes Command security policies, responsibilities and procedures. In the absence of specific reference to Command requirements herein or in other separate directives, the provisions of reference (a) apply.

0102. SECURITY PRINCIPLE

Security is the direct, immediate, legal and moral responsibility of every person in the Department of the Navy. The term "person in the Department of the Navy" is defined to include all persons in the naval service and civilians employed by the Department of the Navy. The security principle employed by the Department of Defense is based on circulation control; i.e., control of dissemination of classified information. This principle is designed to limit knowledge or possession of classified information to persons whose duties and "need-to-know" require such access in the interest of defense and who have been investigated and determined to be trustworthy.

0103. COMMAND RESPONSIBILITY AND AUTHORITY

The Director of Security is responsible to the Commander, Space and Naval Warfare Systems Command to administer the overall security program within SPAWAR Headquarters and to provide security direction to SPAWARSYSCOM Activities.

1. The Division Director, Information Security Division (SPAWAR 10H1) is designated as the SPAWAR Security Manager and is responsible for formulation, implementation, and enforcement of security policies and procedures for the protection of classified information originated by and/or under the cognizance of SPAWAR/SPAWAR contractors. In connection with these duties, disclosure of classified information is authorized and access to all areas shall be given to appropriately identified representatives of the Security Office during the conduct of investigations and inspections.

a. The Security Manager shall be assisted by:

(1) The Head of Mail Records and Printing Branch (SPAWAR 18-51), who shall be responsible for uniform compliance with Secret and Confidential classified information handling procedures within SPAWAR.

b. The Top Secret Control Officer (SPAWAR 00H), and appointed alternate, who shall establish uniform compliance and handling procedures and accountability for Top Secret information within SPAWAR.

c. Security Coordinators, as designated in accordance with Chapter 2, Section 6, who shall act as liaison between the Security Office and their area of jurisdiction and perform such other functions as prescribed herein.

2. The Division Director, Computer Security Division (SPAWAR 10H2) is designated as the SPAWAR Automated Data Processing Security Manager (ADPSM) and is the single focal point for SPAWAR operational automated information system (AIS) security program implementation matters. The SPAWAR ADPSM acts as the agent for the SPAWAR Designated Approving Authority (DAA) and is the SPAWAR HQ ADP Security Officer (ADPSO). The ADPSM is responsible for the general management, administration, coordination and monitoring of the SPAWAR AIS security program.

3. The Division Director, Physical and Operations Security Division (SPAWAR 10H3) is designated as the SPAWAR Security Officer. The Security Officer is responsible to manage, implement and direct the SPAWAR physical security, anti-terrorism, and loss prevention programs, coordinate security requirements of tenant offices/activities and ensure liaison is maintained with civil and military officials. Organizational Security Coordinators, designated in accordance with Chapter 2, will assist the Security Officer.

CHAPTER II

HEADQUARTERS/BUILDING SECURITY

SECTION 1

CONTROL OF CLASSIFIED MATERIAL

0201. GENERAL

All classified material originated or received by SPAWAR shall be recorded, processed and protected as outlined herein, unless specific deviation is authorized in writing by the Security Office.

0202. ACCESS TO CLASSIFIED MATERIAL

Access to classified material shall be limited to those persons who require access for the performance of official SPAWAR duties and who have been investigated and cleared in accordance with current standards for the degree of access required. Responsibility for determining the "need-to-know" and security clearance rests with the holder of the information and not with the prospective recipient.

0203. SPAWAR CENTRAL CLASSIFIED MATERIAL CUSTODIAN

Accountability for and control of classified material, and other accountable documents, begins with their origin or receipt in SPAWAR. SPAWAR 18-51 is the central custodian and is responsible for overall control of Secret and Confidential material within SPAWAR. SPAWAR 00H controls all Top Secret material originated and received by this Command.

0204. ACCOUNTABILITY AND CONTROL

All Secret and Top Secret material shall be recorded. Such classified material received directly by any individual in SPAWAR from any source shall be delivered to SPAWAR 18-512 or SPAWAR 00H, as appropriate, immediately for recording. The circulation and movement of all material by custodians, unless specifically exempted by the Security Office, shall be as follows:

1. Top Secret Information

a. SPAWAR 00H has been appointed Top Secret Control Officer for SPAWAR Headquarters, except for the WWMCCS Site located at the Washington Navy Yard which is addressed in subparagraph I. below. The dissemination of Top Secret information within SPAWAR shall be strictly controlled by SPAWAR 00H and limited to persons possessing a real "need-to-know". The person receipting for the Top Secret information shall ensure complete accountability at all times.

b. Top Secret information received from sources other than SPAWAR 00H shall be immediately delivered to SPAWAR 00H for proper accountability.

c. Top Secret material may be checked out from SPAWAR 00H by persons having proper security clearance and "need-to-know". Material may be viewed in SPAWAR 00H spaces by anyone having proper clearance and "need-to-know" as ascertained by SPAWAR 00H. Standard Form 703 will be attached to cover each Top Secret document.

d. Top Secret material shall be returned to SPAWAR 00H prior to 1500 hours daily. Exceptions to this requirement may only be made by SPAWAR 00H, only if absolutely essential and only if adequate storage is available.

e. When Top Secret information is to be originated or prepared, SPAWAR 00H shall be contacted prior to commencing. SPAWAR 00H will assign an accountability number and issue a disclosure sheet and a residue envelope. All rough drafts, scraps, typewriter ribbons, etc. will be placed in the residue envelope and returned to SPAWAR 00H along with the smooth copies. Numbering and marking shall be in accordance with reference (a).

f. Top Secret information shall not be reproduced without the approval of SPAWAR 00H.

g. Destruction of Top Secret information is the exclusive responsibility of SPAWAR 00H.

h. The processing of Top Secret data in computers, automated information systems and networks is prohibited unless the system or network has the proper security accreditation.

i. PD 620 is responsible for Top Secret Control at the CNO/SPAWAR WWMCCS Site at the Washington Navy Yard. PD 60 will appoint, in writing, a Top Secret Control Officer to perform this duty. The Security Office (SPAWAR 10H) will exercise oversight of all control activities performed by this position.

2. <u>Secret Information</u>

a. A computerized bar code based document control system has been developed for accountability of all Secret material within SPAWARHQ received and processed through SPAWAR 18-5 in National Center #1 (NC-1). The system will be comprised of central processing stations located in the Mail Room (SPAWAR 18-51) with subordinate stations located in primary classified material custodians offices throughout NC-1. All Secret material received, generated, internally transferred, dispatched, or destroyed will be processed through this system. When all documents have been bar coded and recorded in the database, internal document transfers will be accomplished between custodians through use of a bar code scanner. Custodians will continue to sign for Secret material under the new system.

NOTE: Each document in a multiple document package receives a different b code number. However, documents are perforated with the lead docum bar code number for tracking purposes.

b. All offices shall establish an intra office system of control will provide a continuous chain of receipts clearly trackable to the holde the material. Standard Form 704 will be used to cover each Secret documen

c. When Secret material is originated for transmittal, a serial n shall be obtained from SPAWAR 18-512. Material shall then be prepared for transmittal in accordance with the provisions of paragraph 0213 and hand delivered to SPAWAR 18-512.

d. When directed by the Security Office, SPAWAR 18-51 will reques offices to submit an inventory of Secret documents on hand, based on a phy examination of each document. This inventory will be balanced against SPA 18-512's record of official custody. Discrepancies which cannot be resolv SPAWAR 18-51 and the office involved shall be referred to the Security Off

3. Confidential Information

a. For internal security control purposes, mail logs are not requ When required for mail control purposes, however, mail clerks shall ensure no classified information is included in the mail logs.

b. A Confidential Route Sheet (SPAWAR 5511/3) and Confidential Co Sheet (Standard Form 705) will be affixed to all Confidential material rec (except messages) by SPAWAR 18-511 prior to routing. Offices receiving Confidential material will provide security protection for all Confidentia material received, originated, transmitted or stored to the extent require this manual. Mail addressed personally to individuals will not be opened SPAWAR 18-511. It is the responsibility of all offices receiving personall addressed mail from SPAWAR 18-511, or any other sources, to ensure that su mail is delivered to the addressee and examined to determine if Confidenti information is contained therein. Unopened First Class Mail will be prote as Confidential unless known to contain only unclassified material. (This requirement is imposed since Confidential material addressed to Department Defense activities in the United States and its territories may be sent Vi First Class Mail.)

4. Classified Messages

a. Top Secret messages are handled in the manner described above. Incoming Secret and Confidential messages are received from the Naval Communications Center, Crystal Plaza, along with unclassified messages. T only identification that a message is classified is the word SECRET or CONFIDENTIAL at the head and foot of each page of the message and in the f

line of the text. Generally, the size and color of this marking is the same as the text. These messages are received by SPAWAR 18-512 pre-routed and are not controlled prior to receipt by SPAWAR.

b. Confidential messages are delivered to the action office indicated with no special route sheets or classification indicators. It is the responsibility of the office receiving messages to examine each one carefully and affix a Confidential Material Control Record (SPAWAR 5511/3) and a Confidential Cover Sheet (Standard Form 705) to those that are Confidential.

c. Secret messages will be separated by SPAWAR 18-51 and routed as Secret documents. Each Secret message will be protected as indicated in paragraph 0205.2.

5. COMTAC Publications (Tactical)

a. COMTAC publications may be checked out from SPAWAR 18-53 during normal hours by signature, on a "need-to-know" basis, by any SPAWAR employee who has appropriate clearance. Publications may not be checked out on a permanent retention basis and are subject to recall by SPAWAR 18-53. Publications will normally be returned to SPAWAR 18-53 within a 2-week period. When "need-to-know" cannot be determined by SPAWAR 18-53, a written justification signed by the cognizant Division Director is required.

b. All material in COMTAC publications, regardless of classification, is considered privileged information and, if unclassified, is to be treated as For Official Use Only. The person who has drawn a COMTAC publication is personally responsible for the accountability, safeguarding, and maintenance of the publication. He/she is responsible for entering all changes while the publication is in his/her custody. COMTAC publications must be hand-carried to and from SPAWAR 18-53.

6. Communication Security (COMSEC)

a. COMSEC publications require strict control. Eligibility for access is determined by SPAWAR 18-2 on a case-by-case basis. In addition to the requisite clearance and "need-to-know", the recipient must be familiar with the COMSEC system. (SPAWAR 18-2 will provide briefing on the COMSEC system, as required.)

b. Prior to release of any COMSEC Material System (CMS) material to a firm under contract to SPAWAR, the project manager/engineer shall submit a request to the Security Office for review. The request shall include sufficient justification upon which to base a decision that such release is in the best interests of the Navy and a statement that all applicable requirements of this paragraph and reference (a) have been met. Additionally, the following information, as applicable to the specific situation, shall be included in the request:

(1) Contract number, contractor name, facility clearance, and location at which the function will be performed.

(2) Nature and scope of the contractual functions; the COMSEC information, material, or equipment to which the contractor personnel will have access; and the number of contractor personnel involved.

(3) In the case of contractor operation of a secure telecommunications facility, the classification and type of material involved and whether access to U. S. Government traffic will be supervised by Government civilian or military personnel.

(4) The initial date on which contractor personnel will have access to COMSEC information, material, or equipment and the length of the contract or period of time such access will be required.

(5) Description of any additional administrative or security measures over and above the requirements of this paragraph or of reference (a) or OPNAVINST 2221.5, which will be implemented to ensure that contractor personnel will not gain access to classified information or material for which they do not possess a security clearance and valid "need-to-know".

(6) The Security Office will forward all appropriately justified requests to COMNAVSECGRU for final approval.

0205. CLASSIFIED MATERIAL CONTROL RECORD (ROUTE SHEETS)

A series of forms have been developed to serve as a cover sheet and internal routing form. These forms are in three distinctive colors which designate the classification of the material attached. Within SPAWAR, all classified information being routed, inter or intra-office, or when otherwise subject to unauthorized visual access, shall be covered by the forms indicated below:

1. Confidential. Confidential Material Control Record (SPAWAR 5511/3) and Standard Form 705.

2. Secret. Secret Material Control Record (SPAWAR 5511/2) and Standard Form 704.

3. Top Secret. Top Secret Control Record (OPNAV Form 5511/13)and Standard Form 703.

0206. RETAINING OR COPYING CLASSIFIED DOCUMENTS

1. Top Secret and Secret documents shall not be detached from routing sheets or duplicated without the prior authority of SPAWAR 00H or SPAWAR 18-512 as appropriate. Additionally, duplication shall be subject to specific instructions provided by the originator.

2. Material classified Secret, originating outside the Department of Defense will not be reproduced without the consent of the originating agency. All Secret material to be reproduced will be delivered to SPAWAR 18-512. SPAWAR 18-512 will duplicate and record the Secret material and release it to the requesting office upon obtaining properly signed receipts. Exceptions to the above procedure may only be authorized by SPAWAR 18-51 or the Security Office when justified. An exception to this procedure is permitted for working papers. Offices reproducing working papers for intra-office use shall establish strict accountability controls and ensure full compliance with paragraph 0208.

3. Requests for reproductions of Top Secret material will be made to the Top Secret Control Officer (SPAWAR 00H).

4. Each office shall institute procedures to monitor copying of classified information that will ensure copying is absolutely essential and limited to exact quantities required for the task involved. Individuals reproducing classified material shall be thoroughly familiar with the classified reproduction rules outlined in this manual.

0207. HANDLING PRECAUTIONS AND OFFICE PRACTICE

The following precautions shall be observed by SPAWAR personnel to prevent deliberate or casual access to classified material or information by unauthorized persons:

1. Keep classified documents in a stowage container when not in use. When removed for working purposes, keep covered when not in actual use.

2. If it is necessary to vacate the office, all classified material shall be returned to its stowage container and locked, or left in custody of persons cleared for access to the subject matter.

3. Receive visitors in areas devoid of classified materials whenever possible, unless the purpose of the visit is to discuss such materials.

4. Protect all working material containing classified information, such as rough drafts, carbon paper, stencils, stenographic notes, paper, and typewriter ribbons, in the same manner as original classified documents until no longer required and destroyed.

5. Do not discuss classified information over the telephone or internal communications systems, unless approved for classified use (e.g., STU-III's).

6. Immediately report any loss, compromise or suspected compromise to the Security Office. During non-working hours, report to the SPAWAR Duty Officer.

For classified documents lost in travel status where no U. S. Military Activity exists in the area, notify the nearest Naval Security and Investigative Command (NSIC) Regional Office or FBI Field office as well as SPAWARHQ by the quickest means possible.

0208. CONTROL OF CLASSIFIED WORKING PAPERS OR PRELIMINARY DRAFTS

1. The terms include, but are not limited to, the following:

All written material whether handwritten, printed or typed; magnetic recordings, all photographs, negatives, exposed or printed films, all punched cards, magnetic, diskettes, disk packs or tapes, carbon paper, typewriter ribbons in connection with the handling, processing, production, and utilization of classified information. Working papers containing classified information shall be:

a. Dated when created.

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

c. Protected in accordance with the classification assigned.

d. Destroyed when they have served their purpose.

2. Such documents shall be recorded with SPAWAR 18-512 or destroyed when the first of any of the following events occur:

a. The document is retained after the next successive stage in its development is completed (e.g., notes converted to draft, final draft placed on master, etc.).

b. The document is retained as a completed document for more than 90 days from the date of origination.

c. The document is reproduced for external purposes (e.g., draft, review, coordination outside the originating code) prior to preparation of final copy.

d. The document, regardless of stage development, is transmitted outside SPAWAR for retention by the receiving office. Any deviation from this guidance must be approved by the Security Office.

3. Top Secret working papers shall be prepared and controlled as directed by SPAWAR 00H.

0209 DISTRIBUTION LISTS FOR CLASSIFIED DOCUMENTS

All personnel who originate classified documents shall prepare and review distribution lists in accordance with this paragraph.

1. The preparer of the distribution list must determine that all prospective recipients (government and non-government) have a valid requirement for access to the classified information involved. This determination will be based upon an evaluation of the contents of the document and a knowledge that possession of the document by the recipients would meet an operational need of SPAWAR or the Department of Defense.

2. Before including a contractor on the distribution list, the preparer will verify that the contractor has the ability to safeguard the level of classified information involved and the information is required in support of a DoD contract or approved program. This verification will be obtained from SPAWAR 10H by providing the contractor's name, address and a description of the material to be released.

3. Distribution lists will be reviewed by the originator semi-annually and whenever a revision to a classified document is prepared. At this time, any previous recipient who no longer meets the requirements of subparagraph 1. above will be deleted from the list. Such deleted recipients will be advised to destroy the copies of documents that they hold. Exhibit 2-18 is a format that will be used for this purpose.

4. Distribution lists will be periodically reviewed by SPAWAR 10H to ensure full compliance with this instruction.

SECTION 2

TRANSMISSION

0210. GENERAL

Classified material including magnetic media shall only be removed from SPAWAR when required for official purposes. The following methods and procedures are authorized:

1. Classified material may be transmitted by SPAWAR Central Classified Material Custodian and/or Top Secret Control Officer via official channels and approved methods (see paragraph 0213).

2. Classified material (except in the Top Secret category) may be hand-carried (using surface transportation only) by appropriately cleared SPAWAR employees to an activity in connection with official duties, provided:

a. Supervisor's approval is obtained. Supervisors are to ensure that the individual fully understands all requirements and that the conditions of this Section have been met prior to granting approval. Courier authorization may be issued by supervisory personnel with "By direction" authority using the format of Exhibit 2-1. <u>There will be no blanket courier authorization issued.</u> The original courier authorizations are to be retained by the individual. A copy of the authorization will be provided to the guard at the time of inspection. The guard will provide the copy to SPAWAR 10H for appropriate verification. No classified material is to be removed from the building without proper authorization. Personnel discovered carrying classified material without written authorization will be detained until SPAWAR 10H is notified and takes charge of the situation. The following conditions must be met:

(1) A determination is made that the necessary classified material is not available at the activity involved.

(2) Time does not permit the material to be transmitted by normal channels.

(3) Appropriate correspondence, serialized and dated, is prepared and processed to SPAWAR 18-512 in accordance with paragraph 0213.2. (This applies to Secret material only. Confidential material need not be processed through SPAWAR 18-512 but must meet all other requirements for Secret.) (<u>NOTE</u>: When classified material is removed for temporary use within the Washington, DC metropolitan area and is to be returned to SPAWAR's custody within the same day, such removal is not subject to the provisions of this subparagraph. All

other provisions of this section will apply. When classified material is removed under these conditions, a list of the material being carried must be maintained by the individual's Classified Material Custodian and an accounting conducted immediately upon return by the custodian. Any discrepancies, including loss and/or possible compromise, shall be reported immediately to the Security Office.)

(4) The classified material must not be opened, read, studied, displayed or used in any manner in public places or conveyances.

(5) When classified material is carried in a private, public or Government conveyance, it shall not be stowed in any detachable storage compartment such as trailers, luggage racks, etc.

(6) The classified material shall be in the physical possession of the individual at all times if proper stowage at a U. S. Government activity or appropriately cleared contractor facility is not available. Classified material shall not be left in such places as locked automobiles, hotel rooms, hotel safes, train compartments, private residences, public lockers, etc.

(7) When return of the classified material is required, the traveler shall request the activity to return the material via appropriate mail channels. If the activity retains Secret material, the traveler is required to obtain a receipt which shall be delivered to SPAWAR 18-512.

0211 HAND-CARRYING CLASSIFIED INFORMATION ON COMMERCIAL AIRCRAFT

1. Under no circumstances will Top Secret material be carried aboard commercial passenger aircraft flights.

2. Hand carrying of Secret and Confidential material on commercial aircraft is prohibited unless specifically approved by a Flag Officer in the chain of command. Requests will only be approved when the urgency clearly outweighs the potential danger of subjecting the classified material to possible compromise, i.e., extremely serious impediment to a SPAWAR project which would directly and adversely affect national security.

3. When, after consideration of the foregoing, it is considered necessary to hand carry classified information aboard commercial aircraft, a request (over the Flag Officer's signature) fully justifying the need shall be sent to the Security Office containing the following details:

a. Complete justification as to need

b. A statement that military aircraft is not available

c. Name of traveler and rank

d. Classification and volume of material involved

e. Name of airline

f. Flight number

g. Scheduled departure and arrival time

h. Flight route (stops, etc.)

i. Return flight data if it is necessary to hand-carry the classified material back to Washington, D. C.

4. Procedures for Carrying Classified Documents

a. Persons carrying classified documents are to process through the airline ticketing and boarding procedure in the same manner as all other passengers, except for the following:

b. The passenger shall present himself at the screening station for routine processing. The classified documents being carried shall contain no metal bindings and shall be contained in sealed envelopes. Should such envelope be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening official should be able to inspect the envelopes by flexing, feel, weight, etc., without any requirement for opening the envelopes themselves.

c. In the event that the screening official is not satisfied, the passenger at that time shall inform the official that the envelopes contain classified material, and shall exhibit an official U. S. Government identification card, plus separate travel authorization and the authorization by the Security Office (see Exhibit 2-2).

d. At that point, the screening official will process the envelopes with a detection device.

(1) If no alarm results, the envelopes require no further examination.

(2) If an alarm results, the passenger shall not be permitted to board and, therefore, is not subject to further screening for boarding purposes.

e. Opening or reading the classified documents by the screening officer is not permitted.

5. Procedures for Carrying Classified Material in Packages

a. Classified material in sealed or packaged containers, because of size, weight, or other physical characteristics, not suitable for processing under 0211.4.a, shall be processed as follows:

b. The Government official who has authorized the transport of the classified material shall notify the appropriate air carrier in advance of this situation.

c. Upon arriving at the terminal, the passenger carrying the material shall report to the affected airline ticket counter prior to boarding, present his documentation, and the package or cartons to be exempt from screening (see Exhibit 2-2). The airline representative will review the documentation and description of the containers to be exempt. The official may make a telephone call to a representative of the authorizing official, as shown on the letter of authorization, for additional verification.

d. If satisfied with the identification of the passenger and his documentation, the official will provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection. The passenger and other type items he/she may be carrying shall continue to be subject to routine screening.

e. If the airline official is not satisfied with the authenticity of the passenger and his documentation, the passenger will not be permitted to board, and, therefore, is not subject to further screening for boarding purposes.

6. Documentation.

a. Persons carrying envelopes, as provided in paragraph 0211.4a above, shall have a picture identification card and travel authorization which specifically describes the envelopes carried which contain classified information.

b. When authorized to carry packages (paragraph 0211.5 above), Government personnel shall present an identification card or credential carrying a photograph, descriptive data of the individual. (If the identification card does not carry descriptive data, i.e., as a minimum date of birth, height, weight and signature, these items must be included in the letter of authorization.)

c. SPAWAR personnel shall present their DoD building pass.

d. The courier shall have the original of a letter authorizing the individual to carry classified material. A reproduced copy is not acceptable;

however, the traveler shall have sufficient authenticated copies to provide a copy to each airline involved. The letter shall be prepared in accordance with Exhibit 2-2.

e. Classified material must be in sealed envelopes in accordance with standard transmission procedures (paragraph 0210.2).

f. Personnel should carry a state drivers license or other civilian identification in addition to their Armed Forces or Civilian DoD Identification Card.

0212 HAND-CARRYING CLASSIFIED MATERIAL OUTSIDE CONUS

Approved couriers, when traveling across international borders, shall request assistance of U. S. Military or State Department representatives in cases of emergencies or possible customs inspections, respectively, which threaten the security of classified material. Normally, the written authorization provided by the Security Office shall be sufficient to clear customs.

0213 TRAVEL OF PERSONNEL HAVING KNOWLEDGE OF SENSITIVE INFORMATION AND PERSONAL CONDUCT IN THE EVENT OF HIJACKING

1. When deemed appropriate by higher authority, i.e., SPAWAR 00, Deputy and Assistant Commanders, and Program Directors may restrict personnel who have knowledge of extremely sensitive information or substantial amounts of highly classified information from utilizing commercial aircraft. In all cases, these personnel should first consider the availability of military aircraft. The determination to restrict commercial aircraft travel shall be an individual judgement based on the nature, classification and scope of the individual's knowledge, and the overall risk (geographic area, international situation) involved, and the official urgency of the situation.

2. Personal Conduct. In the event a SPAWAR employee is a passenger aboard a commercial aircraft which is hijacked and lands in a foreign country, he shall conduct himself as follows:

a. If identification is requested and the individual is in uniform, he should show an Armed Forces Identification Card. If in civilian clothing, he should show a civilian identification card initially; however, if asked directly if he is in the armed forces, he should not attempt to deny military affiliation.

b. Personnel should not, under any circumstances, reveal any classified information.

c. If questioned or interrogated in the foreign country, common sense and judgement should be used in any response. The phrase "no comment" should be used to answer questions concerning official matters.

d. Upon return to U. S. control, official U. S. investigators may want to debrief detainees. Hence, personnel should observe and mentally note, methods and procedures used by the detainer during their stay in the foreign country.

e. If queried by news representatives upon return to U. S. control, personnel may state name, rank, unit of assignment and home address. They should exercise common sense and judgement in response to other press queries and should use extreme care to avoid any response to questions relating to official matters.

f. If personnel have been given permission to hand-carry classified material, they should keep it on their person and try not to call undue attention to it or themselves. They should not attempt to hide the material aboard the aircraft as sealed envelopes found in the passenger compartments are more likely to be opened and read than those in the physical custody of a person. Any attempt to destroy the material would call undue attention to the carrier and could be dangerous to the safety of the other passengers aboard the aircraft.

g. If, as the result of hijacking, classified material is compromised or subjected to compromise, or there are indications of attempts at foreign intelligence exploitation, the Security Office shall be notified immediately.

0214 TRANSMISSION AND PREPARATION

1. Approved Methods of Transmission

a. Top Secret. As directed by the SPAWAR Top Secret Control Officer (SPAWAR 00H).

b. Secret

(1) The Armed Forces Courier Service (ARFCOS) may be used if the material is qualified in accordance with OPNAVINST 5130.2. Other Secret material may be introduced into the ARFCOS only when the control of such material cannot otherwise be maintained in U. S. custody. (Material such as unclassified correspondence, personal items, etc., are strictly prohibited from entering into ARFCOS.) SPAWAR 00H is the Command's contact with ARFCOS.

(2) Appropriately cleared military and civilian personnel.

(3) Appropriately cleared contractor employees for transmission within U. S. boundaries. In overseas areas, contractor employees may transmit Secret material, within national borders only, when it is necessary for the contractor employee in the performance of a contract project or mission, to remove the classified information from a U. S. Government activity. The material must remain the employee's physical possession and custody at all times and not be stored outside of a U. S. Government activity.

(4) U. S. registered mail, provided the material does not at any time pass through a foreign postal system (except Canadian, as noted in (5) below: Registered mail in the custody of a transporting agency of the U. S. Army, Navy, Air Force or civilian postal system is considered within a U. S. Government control unless the transporting agent is foreign controlled or operated.

(5) U. S. registered mail (registered by a U. S. postal facility) with registered mail receipt between U. S. Government and/or Canadian Government installations in the United States and Canada.

(6) Within United States boundaries only, qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the DoD Industrial Security Program. This method is authorized only when the size, bulk, weight, nature of the shipment, or escort considerations make the use of the foregoing methods impractical. Routings for these shipments will be obtained from the Military Traffic Management Control.

(7) Government carriers under escort of appropriately cleared personnel. Carriers included are Government vehicles, aircraft, ships or the U. S. Fleet or civil service manned U. S. Naval ships. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft may be designated as escorts provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observations or stowage in accordance with Section 5 to prevent inspection, tampering, pilferage or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment which is not accessible to any unauthorized persons aboard, or loaded in specialized shipping containers, including closed cargo containers. Use of specialized containers aboard aircraft requires that:

(a) Appropriately cleared personnel maintain observation of the material while it is being loaded aboard the aircraft and that observation of the aircraft continues until it is airborne.

(b) Observation by appropriately cleared personnel is maintained at the destination while the material is being off-loaded and at any intermediate stops. Observation will be continuous until custody of the material is assumed by appropriately cleared personnel.

(8) Electrical means over approved communication circuits.

c. Confidential

(1) United States Postal Service First Class Mail between Department of Defense activities anywhere in the United States and its Territories..

(2) United States Postal Service certified mail or, if appropriate, registered mail for material directed to DoD contractors and non-DoD agencies of the Executive Branch.

(3) United States Postal Service registered mail; (a) for NATO Confidential material; (b) to and from FPO or APO addressees; (c) to other addressees when the originator is uncertain that their location is within the United States.

NOTE: Confidential mail intended for overseas locations will always be addressed in accordance with the Standard Navy Distribution List (SNDL). Such mail will never be addressed to an overseas geographical location.

(4) Within the United States, commercial carriers which provide a Signature Security Service (SSS).

(5) In the custody of commanders or masters of ships of U. S. registry who are U. S. citizens. Confidential material carried on ships of U. S. registry may not pass out of U. S. Government control. The commanders or masters must receipt for the cargo and agree to: (a) deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo which would be subject to customs inspections will not be unloaded; and (b) maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

2. Preparation (See Figure 1)

a. United States Postal Service First Class Mail between Department of Defense activities anywhere in the United States and its territories shall be prepared for transmission as follows:

(1) The inner and outer envelope of all Confidential mailings must bear the Command's return address.

(2) The outer envelope, to include mailing labels of all Confidential mailings, must bear the notations "POSTMASTER - DO NOT FORWARD, RETURN TO SENDER" and "FIRST CLASS" below the indicia. (NOTE: The envelope for Confidential First Class Mail shall be sealed by the originating office and delivered to SPAWAR 18-511 for mailing.)

b. Whenever classified material is to be registered or certified, as provided above, it shall be hand delivered to SPAWAR 18-512 and prepared for transmission as follows:

(1) With two unsealed opaque envelopes, one inner and one outer. (NOTE: Confidential and Secret material for hand delivery within the Crystal City Complex does not require double envelopes provided other suitable containers are used that will prevent visual observation.)

(2) The inner envelope shall show the address of the receiving activity, the Command's return address, classification and, where appropriate, any special handling requirements.

(3) The outer envelope will be properly addressed, including sender's address and code, but shall not bear a classification marking or any other indication that the contents are classified.

(4) A receipt form (OPNAV Form 5511/10) shall be attached for all Secret transmittals. Confidential material requires a receipt only if the originator deems it necessary. (Receipts for Secret material are prepared by the SPAWAR Central Custodian. Receipts for Confidential material, if required, are prepared by the originating office.)

(5) Mailing labels will be accepted in place of envelopes for multiple distributions.

c. All registered and certified classified material for mailing shall be packaged by SPAWAR 18-512 as follows:

(1) Written material will be folded or packed in such a manner that the text will not be in direct contact with the inner envelopes or container.

(2) Both envelopes shall be carefully sealed to minimize the possibility of access without leaving evidence of tampering.

20 DEC 1988

MAILING OF CONFIDENTIAL MATERIAL

DESTINATION	MAILING METHOD	PREPARATION	STOWAGE CAPABILITY/ SECURITY CLEARANCE
DOD ACTIVITIES IN UNITED STATES & TERRITORIES	FIRST CLASS	DOUBLE WRAPPED	N/A
OTHER EXECUTIVE BRANCH ACTIVITIES IN UNITED STATES & TERRITORIES	CERTIFIED	DOUBLE WRAPPED	N/A
DOD CONTRACTORS IN UNITED STATES & TERRITORIES	CERTIFIED	DOUBLE WRAPPED	VERIFY WITH SECURITY OFFICE IF NOT KNOWN
APO/FPO ADDRESSEES STATE DEPARTMENT POUCH (SEE NOTE BELOW)	REGISTERED	DOUBLE WRAPPED	N/A

OTE: CLASSIFIED MATERIAL WILL NOT BE TRANSMITTED IN SUCH A WAY THAT IT WILL ENTER THE INTERNATIONAL MAIL SYSTEM. ONLY ADDRESSES SPECIFIED IN THE SNDL FOR CLASSIFIED MATERIAL WILL BE USED FOR OVERSEAS TRANSMITTALS.

FIGURE 1

Section 3

OFFICE CLASSIFIED MATERIAL CUSTODIAN

0215. DEFINITION

Office classified material custodians are those designated employees whose duties include responsibility for receiving, controlling, and inventorying all classified material for an organizational element. In other words, they are responsible for the maintenance of the receipt, dispatch and accountability records of classified material.

0216. CRITERIA FOR SELECTION

The responsibility placed on a classified material custodian and alternates requires that careful consideration be given to the qualifications of employees assigned these duties. Assignment should be made only to employees who meet the following criteria:

1. Mature judgement

2. Ability to accept responsibility

3. Initiative to follow and enforce established procedures

4. Previous experience in handling classified material, if possible.

Adherence to these criteria will normally preclude assignment of new employees whose capabilities are not known.

0217. TRAINING

In addition to normal basic security indoctrination, employees designated as office classified material custodians (current and future) will be given specialized training to cover the following subjects:

1. Security classification categories and markings.

2. Command accountability system, including receipt, recording, routing, reproduction, transmittal, retirement and destruction.

3. Access requirements.

4. Stowage requirements.

Training material will include a brochure describing step-by-step procedures which the employee may retain for daily reference.

0218 RESPONSIBILITIES

1. Heads of Directorate, Project Office, and Staff Offices shall:

a. Designate, in writing, to SPAWAR 18-512 via the Security Office, a classified material custodian and alternate. Designations shall include a statement that the designee meets the selection criteria of paragraph 0216. Designations are to be kept current.

b. Ensure that all personnel transferring or detaching are processed through the designated classified material custodian prior to departure. Departing classified custodians shall process through SPAWAR 18-512 to ensure all holdings are accounted for.

c. To verify that this requirement is accomplished, the words "AND CLASSIFIED MATERIAL CUSTODIAN" will be added to Block 14 of the Clearance Sheet. Prior to signing this block, the cognizant supervisor will verify, from the Classified Material Custodian, that all classified material in the employee's possession is accounted for. A search for unaccounted for material will be initiated, if required, and SPAWAR 10H will be notified immediately.

2. SPAWAR 18-512 shall:

a. Maintain a list of personnel authorized to pick-up and receipt for classified material.

b. Establish procedures that will ensure release of classified material only to the designated individuals.

3. The Security Office shall:

a. Review all requests to ensure compliance with requirements of this section.

b. Prepare and present the training program outlined above.

c. Monitor the total classified material custodian program for overall compliance with this section and other applicable sections of this manual.

4. Office classified material custodians shall:

a. Become thoroughly familiar with all aspects of this manual regarding accountability, transmisson, etc.

b. Examine each piece of incoming and outgoing material to ensure that all copies, enclosures, or attachments are accounted for at the time of receipt.

c. Return Secret documents to the Central Secret Records Custodian when no longer required.

Section 4

DESTRUCTION OF CLASSIFIED MATERIAL

0219. AUTHORITY

Classified documents and material that are not permanently valuable records of the Government will not be retained for more than 5 years from the date of origin, unless such retention is authorized by and in accordance with the record disposition schedules of SECNAVINST 5215.5C. Each SPAWAR office shall reduce its classified holdings to the absolute minimum required for operational purposes. Disposal and destruction of unneeded classified holdings will be in accordance with SPAWARNOTE 5210.

0220. REQUIREMENTS AND PROCEDURES

1. Confidential and non-controlled Secret material for destruction will be placed in burn bags and delivered to SPAWAR 18-5, Room 1N08, NC-1, between the hours of 1400 and 1500 for disposition. Non-classified waste materials including glass, metals of any kind, or food stuff shall not be placed in the burn bags. Pulpable and nonpulpable waste need not be separated. Each will be marked with code, name of responsible individual, phone number, and classification of the contents. No more than six pounds of material will be placed in burn bags. If the material is of high density, such as computer printouts, double bagging may be required or lesser quantities placed in the bag. The bags have to be handled several times prior to destruction and it is essential that bags not tear or break open during handling. Under no circumstances will torn or damaged bags be accepted.

2. All accountable Secret material shall be returned to SPAWAR 18-512 for destruction and accountability adjustment.

3. Top Secret material shall be delivered to SPAWAR 00H for proper destruction.

Section 5

SECURITY STOWAGE

0221. SECURITY CONTAINER CUSTODIAN

A principal custodian and an alternate will be designated for each security container. This designation will be indicated on Standard Form 700 (Part 1) (Figure 2), and affixed to the inside of the drawer containing the combination lock in the top drawer of barlocked containers. Custodians and other persons listed on Standard Form 700 must possess a valid SPAWAR security clearance for

the category of information stowed in the container. The principal custodian bears primary responsibility for compliance with security procedures relating to the container and its contents.

0222. COMBINATIONS

1. Combinations must be changed when placed in use or when any of the following occur:

a. At least annually, except for NATO and COMSEC containers which shall be changed semi-annually.

FIGURE 2

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PRIVACY ACT STATEMENT ON REVERSE.	1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
	4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
	6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
	9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

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

b. Immediately when an individual knowing the combination no longer requires access.

c. The combination has been compromised or the container has been discovered unlocked and unattended.

d. The container or the padlock is taken out of service. Reset built-in combination locks to the standard combination of 50-25-50. Reset combination padlocks to the standard combination 10-20-30.

2. Only individuals cleared for the highest level of classified material in the container will change combinations. All combinations will be changed by the security coordinator, or persons assigned to assist the coordinator. If difficulty occurs. contact the Security Office for assistance.

3. In selecting combination numbers, DO NOT use multiples of five (5), simple ascending or decending arithmetical series, and personal data, such as birthdays, etc.. Use numbers that are widely separated (at least 11 numbers apart) by dividing the dial into three parts and using a number from each third as one of the combination numbers. DO NOT use numbers 90 to 0 and 0 to 10. Do not use the same combination for more than one container in any one component.

4. To prevent a lockout, have two different people try a new combination before closing the container, or vault door (usually the container custodian and the security coordinator).

5. Immediately after each change, place the combination (Part 2A), records of combinations in a Combination Change Envelope (Standard Form 700) (Figure 2) and deliver it, unsealed, to the Security Office. Envelopes shall be hand-carried by an appropriately cleared individual prior to 1500 on the change date. Combinations will not be changed on Fridays nor the day proceeding a holiday.

6. Combinations will be released by the Security Office only upon official request by a person listed on the change envelope, or by appropriate supervisor. All combinations shall be memorized. The only authorized written record is that which is maintained by the Security Office.

(Offices having large numbers of containers may record combinations thereto, provided such records are protected to the same degree as the classified material involved and access is limited to those personnel listed on the change envelope.) (NOTE: When combinations are recorded, such records shall be marked with the highest classified being protected.)

0223. STOWAGE

When not in actual use or under the immediate surveillance of an authorized person, classified material will be secured in an approved stowage cabinet.

0224. STOWAGE EQUIPMENT

1. Top Secret Information

Top Secret material will be stowed in a GSA approved security container conforming to Federal Specifications for a class 2, 3, 4, 5, or 6 container with a three-position dial type, changeable combination lock. The security cabinet must be located in an area protected by electronic surveillance devices, which must be approved by the Security Office.

2. Secret Information

The containers described above are the minimum acceptable stowage containers for Secret information.

3. Confidential Information

a. The containers listed above and the following are the minimum acceptable stowage containers for Confidential information.

b. Lock-bar filing cabinets/metal filing cabinets with steel lock-bar mounted so as to preclude opening of any drawer when lock-bar is inserted in the keepers, locked with an authorized combination padlock which meets the requirements of current Federal Specifications for the padlock.

c. During working hours, combination padlocks will be given the same protection as the classified material they protect. When cabinets using padlocks are opened, the lock will be placed in the upper drawer to prevent removal or replacement.

4. No other types of equipment will be used without specific approval of the Security Office. When areas need specific safeguards to meet a condition of work or when minimum requirements cannot be met, the head of the office notifies the Security Office in writing. Stowage cabinets for classified material may be requested through normal supply channels. Requests for cabinets shall be routed to SPAWAR 18-5.

Repair or maintenance of stowage containers will be requested from the Security Office. The Security Office shall be notified promptly should any doubt arise concerning the suitability or state of repair of any security stowage containers. Additionally, the Security Office shall be notified at any time a security container is relocated from office to office, or new equipment is assigned, turned into SPAWAR 18-5, etc.

0225. LOCKING PROCEDURES

The use of proper lock procedures in security stowage containers is vital to the protection of the material. Security stowage containers should be locked without haste, and checked by a second person. The following procedures shall be used within SPAWAR.

1. Safe-Files

Safe-files manufactured by several different firms and in many different models are used in SPAWAR. The mechanical arrangement of these cabinets differs between brands and models. A single procedure that will properly secure all models of safe-files follows:

a. Shut all drawers other than the combination drawer. Push each drawer in firmly, as far as it will go.

b. Shut combination drawer. Push in firmly as far as it will go.

c. If lock has "butterfly" mechanism in center of dial, turn counter-clockwise to free dial for locking.

d. Rotate dial in a clockwise direction, at least four complete revolutions.

e. Test each drawer for security by vigorously pulling it several times.

CAUTION: If cabinet is reopened (such as, for stowage of a last-minute paper) ALL of the foregoing steps must be repeated.

2. Lock-bar filing cabinets

a. Lock-bar cabinets used within SPAWAR are intended to provide reasonable protection against surreptitious entry. When securing lock-bar cabinets, care should be taken to see that the bar is properly inserted through all keepers. The combination padlock shall be rotated at least four complete turns in one direction. The shackle should be pulled firmly to ensure that it is properly engaged. Procedures shall be employed by custodians of lock-bar filing cabinets to preclude the possibility of papers protruding out of the drawers when the cabinets are properly secured. Methods employed may include, but are not limited to:

b. The insertion of a bound book in the front of the drawer to prevent individual papers from being removed.

c. The insertion of stiff cardboard, such as file folders, in the front part of the drawer with one flap in the horizontal position above other papers filed in the drawers and other flap in a vertical position at the front of the drawer.

0226. SECURITY DURING EMERGENCIES

1. The securing of classified matter under emergency conditions, such as a fire or bomb alarm, requires the highest degree of individual initiative. Each Program/Directorate will prepare a plan to provide for complete protection regardless of the number of personnel available. A copy of this plan will be provided to the Security Office.

2. The task of securing lock-bar filing cabinets under emergency conditions, for those offices having large quantities of these containers, may be expedited by having the combination padlocks available in the unlocked position. Under these conditions the locks must be stored inside the container.

0227. DAILY SECURITY INSPECTION

All offices shall establish a double check system to ensure that at the end of each normal working day:

1. All classified material is properly stowed in security cabinets.

2. No classified material is left on desks, in desks, tables, files, etc.

3. Diskettes are removed from all computers and, those containing classified information, are properly secured.

4. That all reproduction equipment is secured under paragraph 0206.5.

5. Burn bags are properly stowed.

6. The contents of wastebaskets are checked to ensure they contain no classified material.

7. Classified shorthand notes, carbon paper, rough drafts, and similar papers have been properly stowed. As a matter of routine during the day, such items should be placed in burn bags immediately after they have served their purpose.

8. That typewriter ribbons used in typing classified material are protected in the same manner as required for the highest level of classification for which they have been used. Exceptions are:

a. After the upper and lower sections have been cycled through the machine five times in the course of regular typing, all fabric ribbons may be treated as unclassified regardless of their classified use thereafter.

b. Any typewriter ribbon which remains substantially stationary in the typewriter until it has received at least five consecutive impressions may be treated as unclassified.

9. Stowage cabinets are locked and properly secured. A record of the above assignments and inspections will be maintained using a Security Check List (Standard Form 701). The form will be modified as shown in Exhibit 2-15 to provide for two persons to initial each item on the form. In this way,

double check performance will be documented. A Security Container Check Sheet (Standard Form 702), Exhibit 2-16, will be prominently posted on each storage container.

10. That ignition keys for the STU-III telephone is removed.

11. In order to support improved security surveillance, a Command-wide "Clean Desk" policy is directed. Specifically, this policy establishes the following requirements in all spaces upon completion of business hours and before the final security check:

a. Desks will be clear of all written or printed matter except a calendar and/or a telephone list finder.

b. Tops of tables, credenzas, file cabinets, bookcases, and other furniture shall be clear of all printed matters except books or magazines which are clearly unclassified material.

c. A "Clean Desk" will be required during an individual's non-duty hours.

d. Disks and other removal media are removed from automated information systems and the system(s) are powered down.

e. Typewriter ribbons and printer ribbons are removed or an "UNCLASSIFIED" sticker (available in the Security Office) affixed to the machine.

f. Reproduction machines are cleared by running once and checking the reproduction paper for impressions. The inside of the cabinet housing the reproduction machine should be examined to ensure that no unaccounted for copies have been left inside. Machines will be turned off on weekends and holidays, except when actually being utilized.

g. Telecopiers are cleared.

h. Security container tops are cleared of all matter.

0228. CARE AFTER WORKING HOURS OF STOWAGE CABINETS

Whenever an individual is working alone after 1530 hours on a normal day or anytime Saturday, Sunday or Holiday, and there are open classified containers in the spaces, the Guard or Duty Officer shall be requested to double check the stowage container or alarmed area.

0229. AREAS PROTECTED BY ELECTRONIC INTRUSION DETECTION DEVICES

Electronic alarm systems may be installed on certain sensitive areas as a means of supplementing security. Classified information located within alarmed areas will be protected by the highest standard of security possible. Any deviation from this standard must be approved by the Security Office. Alarmed areas approved by the Security Office for open storage will be limited to open stowage of classified material up to and including Secret. Areas designated as alarmed areas must conform to the following standards.

1. The area must be locked during periods when it is not occupied. During non-duty hours the unoccupied area will be secured by locking all doors with the combination lock and activating the alarm system. During duty hours, doors locked with the combination lock will be considered adequate.

2. Only SPAWAR employees who have a Secret clearance and the "need-to-know" will be permitted in the area without supervision.

3. Uncleared persons, such as cleaning personnel, may be permitted in the area only under continuous escort and close supervision. All classified material on the walls must be covered during the period these individuals are in the area.

4. Maintenance and service personnel (except alarm technicians and cleaning personnel) will not be permitted in the area without Security Office approval.

5. Non-SPAWAR employees, regardless of cleared status, must be under continuous escort by a cleared SPAWAR employee, while in the area.

6. Opening and Closing Alarmed Areas. Individual instructions will be issued by the Security Office to all custodians of areas protected by electronic intrusion devices.

Section 6

SECURITY COORDINATORS

0230. DIRECTORATE, PROJECT OFFICE AND STAFF OFFICE SECURITY COORDINATORS

1. Deputy Commanders, Assistant Commanders, Program Directors, Director of Naval Laboratories, and Heads of Directorates and Staff Offices will nominate to SPAWAR 10H, one individual to serve as a Security Coordinator. Qualifications for this position are:

a. Mature judgement

b. Ability to accept responsibility

c. Initiative to follow and enforce established procedures

d. Previous experience in handling classified material, if possible. Adherence to these criteria will normally preclude assignment of new employees whose capabilities are not known. SPAWAR 10H will, if the nominee is qualified, provide a letter of appointment (Exhibit 2-3). Additional individuals may be appointed, by the nominating officials identified above, to assist the security coordinator in implementing his responsibilities.

2. Security Coordinators are responsible for providing assistance to the Security Office in the overall monitoring of office security practices to ensure compliance with the requirements of this manual. Examples of these requirements and responsibilities include, but need not be limited to, the following:

a. Classification and marking of classified material.

b. Transmission of classified material.

c. Visitor control as it relates to clearances and "need-to-know".

d. Padlock/safe combination control to include instructing personnel on changing procedures and ensuring that combinations are changed when required.

e. Indoctrination of newly assigned personnel.

f. Establishment of a double check system of inspection to ensure security of classified material during and after duty hours.

g. Storage of classified material is limited to authorized containers which are in good mechanical condition.

h. Periodic refresher training is conducted to ensure that all personnel are familiar with their responsibility to safeguard classified material and the "need-to-know" concept is practiced at all times.

3. The Security Office will provide the individuals designated as Security Coordinators with a special security indoctrination upon appointment and an annual refresher briefing thereafter. The Security Office will also assist them in developing any additional security measures applicable.

4. The Security Coordinators are also responsible for identifying sensitive projects or fields of information under their cognizance and to conduct security inspections as outlined by Section 7 of this Chapter.

Section 7

SECURITY INSPECTIONS

0231. GENERAL

The security posture of this Headquarters must be of continued concern to all employees if an acceptable level of security is to be attained. A sound security program is absolutely dependent on the cooperation of all personnel, not only by observing security regulations but also by being responsive to the need to continuously up-grade the level of security. This can only be achieved by identifying and eliminating security deficiencies and weaknesses. The most effective method of accomplishing these objectives is through a system of continuous self-inspections and appraisals.

1. Scope of Inspections

Security inspections shall encompass all facets of security, i.e., physical security, industrial security, personnel security, classification management and foreign disclosures. Inspections will cover working hours as well as non-working hours.

2. Action

a. All personnel, using Exhibit 2-4 as a guide, shall continuously review their security practices with the objective of eliminating security deficiencies and upgrading Command security in general.

b. Security Coordinators (as designated in accordance with Section 6) shall conduct thorough security inspections in their areas of responsibility on an annual basis commencing at the beginning of the calendar year. Inspection reports, following the format of Exhibit 2-4, shall be submitted to the Security Office via the appropriate Directorate or Program Manager.

c. Security Office shall conduct inspections as frequently as deemed necessary to ensure that the Command's security policies are being fully observed. These inspections shall include, but not be limited to, a thorough examination of all office space to determine whether classified material is left adrift, security containers are properly secured, and safe and padlock

combinations are not improperly recorded, e.g., on desk calenders, list finders, in locked desks or in any other unauthorized manner. Additionally, security containers shall be inspected on a random basis to determine if they are being properly used, i.e., do not contain valuable personal items, unrecorded Secret material, etc. Inspections of security containers will normally be conducted during duty hours.

3. Property

a. All property, except for properly documented classified items, are subject to inspection in accordance with Navy Regulations and GSA Directives, prior to entry or removal from the building. Searches of persons will not be made unless accomplished by a law enforcement officer incident to arrest of the persons. Any person observed removing property that is not clearly identifiable as personal property will be challenged and the authority for removal of the property established. Until such authority is established, the property will remain in the custody of the Security Guard or Security Office personnel.

b. The following ingress/egress inspections are authorized as directed by the Director of Security.

(1) Random vehicle inspections, and

(2) Random inspections of hand-carried articles (brief cases, purses, packages, etc.), buildings, and office spaces.

c. The results of all inspections shall be submitted to the Commander for review.

Section 8

SECURITY TRAINING AND EDUCATION

0232. SECURITY EDUCATION

1. It is the policy of this Command to promote a strong and continuing security education program in accordance with reference (a). This program will increase the effectiveness in all personnel, and ensure uniform interpretation and application of security standards. Security education is applicable to all personnel, regardless of their position, rank, or grade.

2. The objectives of the security education program are to:

a. Advise personnel of:

(1) The need for protecting government property and sensitive or classified information.

(2) The adverse effects to the national security resulting from unauthorized disclosure of sensitive or classified information.

(3) Their responsibility for protecting government property and sensitive or classified information in their possession.

b. Familiarize personnel with specific security procedures.

c. Familiarization with procedures for challenging classification decisions.

d. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information and personnel's responsibility for reporting such attempts.

e. Advise personnel of the hazards involved and the strict prohibition against discussing classified information over the telephone or in any manner that can be intercepted by unauthorized persons.

f. Advise personnel of disciplinary action thay may result from violations of security regulations.

3. Responsibility

a. The Director of Security, is responsible for implementing and maintaining an effective security education program. He will ensure that the program does not evolve into a routine compliance with the formal requirements without achieving the real goals of the program.

b. The Security Education and Training Officer, (SPAWAR 10H14) is responsible for formulating and coordinating the security education program and for designing it to fit the particular requirements of the different groups of personnel. This office will also maintain records of attendance for all security training.

c. Department Security Coordinators, (See Chapter II, Section 6) are responsible for ensuring that supervisors and managers under their cognizance are informed of all security briefings. They will maintain an informal record of who attended the briefings.

d. Supervisors will ensure that individuals under their supervision are familiar with the specific security requirements of their particular assignments and work areas. They will also ensure that individuals under their supervision are informed of various security briefings and ensure they attend. Supervisors will also attend a mandatory threat awareness briefing to be presented annually by SPAWAR 10H.

4. Types and Requirements of Security Briefings

a. Orientation Briefings

An orientation briefing will be given to all newly reporting personnel (military and civilian) as soon as possible to ensure that they are aware of the Command's security policy and procedures, and of the basic requirements for the protection of government property and sensitive or classified information. The time, date and location of the briefing will be given to the reporting individual when he or she checks in with SPAWAR. This briefing satisfies the requirement for annual refresher and security presentation for the calendar year in which it is given. In order to ensure the action required above, the following procedure will be followed:

b. Thirty calendar days after a new employee reports on board, the cognizant security coordinator will, through his line supervisor, submit a Security Orientation Certificate (Exhibit 2-5) to the Security Office, signed by the new employee and witnessed by his line supervisor. The certificate will be given to the new employee when receiving the original security orientation from the Security Office.

c. Refresher Briefings. A refresher briefing is required annually for all personnel who have access to classified information. This briefing is coordinated by SPAWAR 10H with the various Command Security Coordinators. The refresher briefing may also be given when a code's record of security infractions and violations indicates a need for such a briefing.

d. Special Briefings. There are various types of special briefings, the responsibilities and/or requirement for which are listed below:

(1) Communication Security (COMSEC) Briefings. These Naval security briefings are the responsibility of the COMSEC Custodian, SPAWAR 18-2C, and are given to COMSEC personnel.

(2) Counterespionage Briefings. All personnel who have Secret or Top Secret clearance shall receive a counterespionage briefing, given by the Naval Security and Investigative Command, at least once every three years.

(3) Foreign Travel Briefings. See paragraph 0605.

(4) Special Access Program Briefing. See paragraph 0413.

5. Debriefings

a. Personnel who have access to classified information must be debriefed by SPAWAR 10H under the following conditions:

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

c. At the conclusion of the access period when a Limited Access Authorization has been granted.

d. When an individual's security clearance is revoked for cause.

e. When an individual's security clearance is administratively withdrawn.

6. Resources

a. SPAWAR 10H is responsible for the following security education resources:

b. That timely security matters of concern to SPAWARSYSCOM personnel are included within Command newsletter.

c. Security Posters are distributed to all department Security Coordinators several times a year. Security Coordinators are responsible for determining how many posters are needed and where they are to be posted to ensure that all personnel in their departments see them. These posters should be placed in picture frames available through the supply system and not attached directly to the walls. Extra posters are available to anyone upon request as long as the limited supply lasts. Any organization not currently on distribution may be added by contacting its Security Coordinator or SPAWAR 10H.

d. Videotapes, Motion Pictures, and Slide-tapes. A supply of these media is maintained for use by SPAWAR personnel in various briefings. To determine what is available, and possible use in security related briefings, contact the Security Education and Training Officer, (SPAWAR 10H14), in Room 1S11.

Section 9

BUILDING SECURITY REGULATIONS

0233. GENERAL

For the purpose of this manual, the term "Building Security" is used to identify the regulations issued by the Department of the Navy for the protection of building spaces or facilities. These regulations are limited to control of access to public areas of the building, property removal, and related matters. Security of classified matter and internal security of spaces occupied by SPAWAR are the direct responsibility of Director, Security Office. The regulations which follow implement OPNAVINST 5500.61 (current series), "Department of Defense Building Security in the Metropolitan Washington, D. C. area", and General Service Administration rules and regulations governing public buildings and grounds and shall be observed by all SPAWAR and non-SPAWAR employees (see Exhibit 206).

0234. SECURITY HOURS AND SIGN IN/OUT PROCEDURES

Security hours at National Center No. 1 are for the full 24-hour period. Duty hours are 0600-1800, Monday through Friday.

0235. ADMITTANCE

1. All personnel must show a valid DoD building pass for admittance. Building passes must be displayed in front, above the waist, on outer clothing at all times while in the building. During duty hours (0600-1800, Monday through Friday) guards stationed in the main lobby and at the garage entrance will deny entrance to anyone not in possession of a DoD building pass. Persons not in possession of DoD building passes will be referred to the Visitor Control Office and issued visitor pass after they have been identified and the point of contact (POC) has verified their need to visit. The following passes are valid for entry to NC-1:

- White DD Form 1466 (DoD Building Pass)
- Pink DD Form 146 (DoD Building Pass)
- Orange DD Form 1469 (Temporary DoD Building Pass)
- SPAWAR NC-1 Pass
- SPAWAR Daily Visitor Pass

a. SPAWAR daily passes will be marked with either the floor(s) on which an individual is authorized to conduct business or a circled "E" indicating that the visitor must be escorted at all times. Visitors without a security clearance on file will have a red line across the center of their daily badge. Daily badges for foreign visitors will be marked with a horizontal green line in addition to a red line.

b. The visitor pass will also indicate the POC and room number to be visited. The floor number to be visited will be indicated by large number(s) on the visitor pass. It is the responsibility of the POC to ensure that if their visitor(s) has business in another office or on another floor, that they are either escorted by them to that office or directed to the Visitor Control Office (VCO) for issue of a new pass. (Escorts for visitors to another floor must remain with the visitor until visit is complete or they must return to the VCO for a new pass.) Visitors who are not escorted, or have not made arrangements with the VCO, will be denied visit privileges.

2. During non-duty hours (Saturday, Sunday Holidays and 1800-0600 Monday through Friday), all pedestrian traffic is channeled through the main street level lobby to be identified by the security guards. The basement level elevator lobby and steel-mesh doors located in both stairwells between the lobby level and second floor will be secured. All doors are alarmed and the general area under CCTV surveillance with motion detection devices. The walkway on the third floor will be permanently closed and alarmed at all times.

3. A steel roll-up overhead door is installed at the entrance to the NC-1 parking garage. This door will be secured only during non-duty hours. Guard control is provided during normal working hours and peak traffic periods. Persons requiring recurring access during non-duty periods may be issued a cardkey which automatically opens the door when inserted in the card reader located at the top of the garage ramp. The door automatically closes once the vehicle has entered the garage. Exiting the garage does not require a cardkey. The door will open automatically. Additionaly, the garage entrance is under CCTV surveillance monitored by the guard force to ensure pedestrians and vehicles do not enter illegally while the door is open for authorized vehicles.

a. Persons with parking privileges and who require regular recurring entrance to the garage during non-duty hours may request a cardkey from SPAWAR 10H by furnishing the information requested by Exhibit 2-17. Requests must be signed by the employee's supervisor. Cardkeys will only be isused to SPAWAR employees requiring access during non-duty hours. (Once a week constitutes regular access.)

b. Persons who infrequently require access to the garage during non-duty hours may make special arrangements with the Security Office. The lobby guard will issue a temporary cardkey during non-duty hours to SPAWAR employees upon presentation of a DoD building pass. In these instances, the cardkey will be turned in to the guard when the individual signs in to the building.

c. When using the cardkey, the individual must first make sure the arrow is facing down and away from the body. The reader will acknowledge the cardkey by a green light. Once the light turns green, the vehicle can then proceed. It takes about five seconds for the door to open and the door remains open for 30 seconds.

d. Should for some reasons the vehicle does not clear the doorway, the door is equipped with a safety device. The foam rubber strip on the bottom of the door requires only a minimum amount of pressure for the door to stop and then go back up. The vehicle will not be damaged.

e. Cardkeys are not transferable. Lost cardkeys shall be reported immediately to SPAWAR 10H.

0236. DOD BUILDING PASSES

All personnel assigned to SPAWAR and all personnel requiring unescorted access to SPAWAR spaces are required to possess a Department of Defense building pass (see Section 10).

0237. PROPERTY PASSES

1. All property carried by persons or in vehicles entering or leaving National Center No. 1 is subject to inspection by the Security Guard or Security Office personnel.

2. Removal of SPAWARSYSCOM property will be in accordance with SPAWARINST 11016.1A and must be approved by the Property Control Administrator (PCA) (SPAWAR 18-52) or a Property Control Custodian (PCC) authorized by the PCA to sign Property Passes (GSA Form 7). A copy of the Property Pass will be surrendered to the Security Guard at time of exit. When the property is returned, the authorizing official, PCA or PCC, will reconcile the Property Passes and retain copies until the next triennial inventory.

3. Non-SPAWARSYSCOM property brought into, or taken out, of the building, as well as property covered by a bill of lading, invoice, sales receipt or other document giving proof of custody or ownership, is exempt from this requirement. A log for the purpose of providing a record of entry and removal from the building will be maintained by the guard for this purpose. Whenever the ownership of property is questioned, resolution will be provided by the PCA.

0238. PHOTOGRAPHIC, VIDEO AND AUDIO RECORDING EQUIPMENT

Non-SPAWAR owned cameras, video, other photographic equipment, audio recording equipment and their use in SPAWAR Headquarters are subject to approval of the Security Office. Request for authorization to use cameras, video, other photographic and audio recording equipment in SPAWAR Headquarters should be submitted, in writing, to the SPAWAR Security Office a minimum of 24 hours in advance. The request should indicate the name of the person who will be bringing the equipment into the building, a list of the equipment to include make and serial number (if any), the justification for its use in SPAWAR spaces, the individual responsible for ensuring its proper use, and when it is expected that the equipment will be taken from the building. When use of the equipment is authorized, the taking of photographs and recording of audio within SPAWAR Headquarters shall be supervised by those in authority at the place or area where the photographs or recordings are taken, to ensure that no classified material is being photographed or recorded and that the proper classification and handling of the film or tapes is complied with. The Security Office will issue a Photographic/Audio Equipment Authorization for use in gaining entry into and removing the equipment from the building.

0239. WEAPONS AND EXPLOSIVES

No person (except an authorized law enforcement officer) entering or while on SPAWARSYSCOM property shall carry or possess firearms, other dangerous or deadly weapons, explosives or items intended to be used to fabricate an explosive or incendiary device.

0240. LOSS OF PROPERTY, THEFTS, AND OTHER IRREGULARITIES

1. Loss or theft of property (Government or personal) will be reported to the Security Office on a GSA Form 182 (Exhibit 2-7) (available in the Security Office). Reported losses will be forwarded to the Defense Protective Service and, as appropriate, other investigative agencies.

2. Persons creating a public nuisance or other irregularities occurring within SPAWAR spaces in NC-1 will be reported to the Guard Office and the Security Office immediately.

Section 10

DEPARTMENT OF DEFENSE BUILDING PASSES

0241. RESPONSIBILITY

1. Washington Headquarters Service (WHS) is responsible for the fabrication and issuance of DoD building passes in the Navy Department administered buildings. Within SPAWAR, the Security Office is responsible for processing the requests for issuance of DoD building passes.

2. Personnel reporting for duty with this Command will report to the Security Office, to be processed for a DoD building pass. When the pass has been received it will be brought to the Visitor Control Office for bar-coding.

3. A favorable National Agency Check (NAC) is required for each person issued a DoD building pass. If a NAC has not been completed, a temporary building pass will be issued pending completion of an NAC.

4. Need for contractor building passes will be scrupulously evaluated based on Command requirements. Sponsorship shall only be undertaken if the contractor requires unescorted access to DoD occupied buildings, other than NC-1, at least three times or more per week in performance of specific contract tasks. Only Assistant Commanders, Program Directors or equivalent are authorized to initiate requests for contractor building passes. When, after consideration of the foregoing policy, sponsorship of a contractor employee for a DoD building pass is justified, Exhibit 2-8 shall be completed and forwarded to SPAWAR 10H.

0242. TYPES OF DOD BUILDING PASSES (PARTIAL LISTING)

1. DD FORM 1466

Issued to DoD personnel, other authorized U. S. Government personnel, DoD consultants, non-Government personnel, DoD contractors and experts who regularly work in, or require frequent and continuing access to DoD buildings. The pass permits access to all buildings or areas as required or designated on the pass.

2. DD Form 1469

A temporary pass for use in a specific DoD building for persons whose presence therein is required for a limited period of time or for persons waiting completion of a National Agency Check. The pass will be issued for only the period necessary and in no case for a period greater than 120 days.

0243. LOSS OF DOD BUILDING PASS

Loss of a building pass will be reported immediately to the Security Office by means of a signed statement (Exhibit 2-9) covering the circumstances involved in the loss. To afford every opportunity for recovery of lost passes, the search for the pass will continue for one week after the signed statement is submitted to the Security Office. If, after thorough search, the pass has not been found, the Security Office will prepare the forms necessary to obtain a replacement. Personnel awaiting replacement passes will be required to register into NC-1, and other buildings within the NCR, as specified in building visitor regulations.

0244. SURRENDER OF BUILDING PASS

Building passes will be surrendered to the Security Office when the following has occurred:

1. Upon transfer or separation of the individual issued the pass.

2. Upon expiration of period of validity. (In this case, the pass will be turned in to the DoD Building Pass Office.)

3. When replacement is requested because of official change of name of bearer.

4. Non-SPAWARSYSCOM holders will surrender their passes to their agency's Security Office for forwarding to SPAWAR.

Section 11

VISITS AND VISITOR CONTROL

0245. VISITOR CATEGORIES

Any person who is not attached to or employed by SPAWAR is considered a visitor. Visitors are divided into the following two categories.

1. U. S. Citizen

Includes military and civilian employees of the U. S. Government, and U. S. citizens representing U. S. commercial and business activities or private interests.

2. Foreign Nationals

Includes any person not a U. S. citizen, immigrant alien or a U. S. national. American citizens representing foreign Governments, foreign private interests, or other foreign nationals are considered foreign nationals for the purposes of this manual. (Chapter 6 outlines detailed procedures for controlling foreign visits.)

0246. VISITS TO SPAWAR

No security clearance is required for unclassified visits by U. S. citizens as defined above. All visits are subject to the concurrence and at the convenience of the person being visited.

1. Security Guidance

a. Personnel Clearances for Visit Purposes

(1) U. S. Government. Personnel security clearances of Government employees are based on formal investigative actions, i.e., National Agency Checks with Written Inquiries (NACI) or Background Investigation (BI). Certifications of employee security clearances by any Agency/Department of the Government are acceptable for access when "need-to-know" requirements are satisfied.

(2) DoD Contractors. Industrial facilities engaged in classified contracts with DoD are authorized to certify their facility and personnel security clearances for visit purposes. There are two types of industrial personnel security clearances. The first type is a clearance issued by the Department of Defense (DoD) based on formal investigative actions, i.e., National Agency Checks (NAC) or Background Investigations (BI). The clearance is issued by the Defense Industrial Security Clearance Office (DISCO), Columbus, OH. The second type is a Confidential clearance issued by cleared contractor facilities to an employee, based on lesser investigative requirements. (NOTE: "Company Confidential" clearances were originally intended for production line employees to utilize their services on classified components in compartmentalized environments which would deny them overall knowledge of classified end items, contracts, or tasks thereunder.) The Industrial Security Manual now permits "Company Confidential" clearances to serve as the basis for visits to military activities and to other contractor facilities. The ease by which birth certificates can be obtained, and thereby serve fraudently to establish citizenship status, renders "Company Confidential" clearances a potentially serious threat to SPAWAR classified information. Accordingly, visits to SPAWAR by persons possessing only "Company Confidential" clearances will be permitted ONLY UNDER EXISTING SPAWAR CONTRACTS AND WILL BE LIMITED TO EMERGENCY ONE-TIME VISITS. Disclosures during such visits will be limited to those necessary to resolve the problem at hand. If the problem requires Confidential disclosures of a broad scope, the contractor will be directed to substitute representatives possessing clearances based on formal investigative actions.

b. Justification for Access

(1) Regardless of the source from which visit requests originate, mere certification of personnel and/or facility security clearances are not, in themselves, adequate for access to SPAWAR classified information. Justification for such access must be provided in order that the "need-to-know" may be determined. It is the responsibility of the employer/sponsor of the visit to furnish such justification. REQUESTS WHICH FAIL TO JUSTIFY THE NEED FOR SUCH ACCESS WILL NOT BE APPROVED.

(2) U. S. Government. The responsibilities and functions of Agencies/Departments of the Government and the position occupied by the prospective visitors within such organizations assist in reaching decisions to permit access to SPAWAR classified information during visits.

(3) Industrial Facilities

(a) SPAWAR Contractors. That a facility has a classified contract with one SPAWAR office does not entitle that contractor to have access to classified information in other SPAWAR areas unless the cognizant office justifies the need for access under its contract to the office to be visited.

(b) Other DoD Contractors. Only the military procuring activity having cognizance of a classified contract with an industrial facility can justify the need for access to classified information of another military activity. Therefore, requests for classified visits which do not contain the procuring military activity's justification ("need-to-know" certification) for need, will be returned to the requestor for resubmission through the procuring military activity.

All disclosures of classified information will be limited to the absolute minimum required to achieve the objectives of which the visit is being made. Information of a sensitive nature will not be disclosed when less sensitive information will meet the desired objective.

2. Responsibility

a. The Security Office will maintain information on commercial activities which may be authorized to receive classified information. The Security Office will also determine the validity of classified visit requests of a broad and general nature and prepare appropriate response to all visit requests that cannot be approved.

b. SPAWAR offices having technical cognizance of the classified information involved in the visit will:

(1) Obtain any additional justification, when required;

(2) Verify from the Security Office the clearance status of the prospective visitor and the facility he represents, when required.

(3) Determine the "need-to-know" for access to the classfiied information involved.

c. Figure 3 - Visitor Control Guide, shall be prominently displayed in all SPAWAR offices and the guidance contained therein followed whenever a visit occurs. Copies of this Guide are available from the Security Office.

3. Procedures

a. All incoming visit requests must be validated by the Visitor Control Office (VCO). Requests that do not contain a current contractor/RFP number, point of contact or a code, purpose, valid expiration date and, in the case of a non-SPAWAR contractor, a "need-to-know" certification (paragraph 0246.1.b(2)(b)), will not be accepted and will be returned to the originator. Exhibit 2-10 will be used by the VCO to inform the point of contact (POC) of the request. If the visit, as requested, is not acceptable, or any limitations are necessary, e.g., different dates, a shorter time period, etc., the point of contact must return the request to the VCO stating the limitations. If the visit is acceptable as requested, the POC does not need to return the request to VCO. Upon arrival, the visitors clearance will be verified, he/she will be issued a visitors badge, and the POC will be notified of his/her arrival.

b. Telephonic visit requests will only be accepted within 24 hours in advance of an emergency visit and will be verified by the VCO. Phone-in visits will not be accepted based on a non-SPAWAR contract unless made by the POC or ACO certifying "need-to-know."

4. Surveillance. To ensure that access is limited to only authorized information, all visitors will be kept under continuous surveillance by the occupants of that space. (All non-SPAWAR employees are considered visitors for the purpose of this requirement.)

5. Visitors' Reports. The Security Office will be notified immediately when any visitor expresses feelings inimical to the best interests of the United States, or any undue interest in information he is not authorized to receive.

FIGURE 3
VISITOR CONTROL GUIDE

CHALLENGE ALL VISITORS *CHALLENGE ALL VISITORS*

VISITOR CONTROL GUIDE

VISITOR CATEGORY	CLASSIFIED VISIT – *WHAT TO DO!*	UNCLASSIFIED VISIT – *WHAT TO DO!*
DOD CONTRACTOR	IDENTIFY, VERIFY SECURITY CLEARANCE* & ESTABLISH "NEED TO KNOW" (MUST BE IN SUPPORT OF A DOD CONTRACT, PRE CONTRACT NEGOTIATIONS OR OTHER APPROVED GOVERNMENT PROGRAM)	IDENTIFY AND ESTABLISH NEED (IDENTITY MAY BE ESTABLISHED BY GOVERNMENT ID CARD, COMPANY ID, DRIVER'S LICENSE)
U.S. GOVERNMENT	IDENTIFY, VERIFY SECURITY CLEARANCE* AND ESTABLISH "NEED TO KNOW" (CLASSIFIED INFORMATION REQUIRED IN PERFORMANCE OF OFFICIAL DUTIES)	IDENTIFY AND ESTABLISH NEED (IDENTITY MAY BE ESTABLISHED BY GOVERNMENT ID CARD, DRIVER'S LICENSE)
FOREIGN	MUST HAVE WRITTEN APPROVAL FROM THE SECURITY OFFICE (SPAWAR FORM 5512/6)	MUST HAVE WRITTEN APPROVAL FROM THE SECURITY OFFICE (SPAWAR FORM 5512/6)
MAINTENANCE, REPAIRMEN, CLEANERS, ETC	NOT AUTHORIZED ACCESS TO CLASSIFIED INFORMATION	VALIDATE NEED AND KEEP UNDER CLOSE SURVEILLANCE AT ALL TIMES
ALL OTHERS	REFER TO THE SECURITY OFFICE	REFER TO THE SECURITY OFFICE

*A VALIDATED VISIT REQUEST FROM THE SECURITY OFFICE MUST BE HELD BY THE PERSON BEING VISITED BEFORE ACCESS TO CLASSIFIED INFORMATION IS AUTHORIZED

IMMEDIATELY REPORT TO THE SECURITY OFFICE (x21622), x28651, 25259) ALL INCIDENTS INVOLVING:

- UNUSUAL BEHAVIOR
- SUSPICIOUS PERSONS
- VISITORS REFUSING TO SHOW ID
- VISITORS SHOWING UNDUE INTEREST IN MATTERS NOT ASSOCIATED WITH VISIT
- VENDORS

NOTE CLASSIFIED MATERIAL WILL NOT BE HANDCARRIED FROM THIS COMMAND WITHOUT PRIOR WRITTEN APPROVAL FROM THE DIRECTORATE/PROJECT AND CLEARED THROUGH THE CLASSIFIED MAIL ROOM (REFER TO SPAWAR-SECURITY MANUAL)

CHALLENGE ALL VISITORS *CHALLENGE ALL VISITORS*

0247. VISITS BY SPAWAR OR SPAWAR SPONSORED PERSONNEL

1. Within Continental U.S. Advance visit notification for SPAWAR personnel to activities of the Naval Establishment, to other DoD agencies, or to industrial facilities requiring access to classified information should be submitted in sufficient time to allow evaluation by the activities being visited. In order to fulfill this Command's responsibility concerning visit clearances, the following procedure will be followed:

a. Preparation of Visit Request

OPNAV Form 5521/27 (Exhibit 2-11) shall be used when furnishing advance visit notification. The originating office shall include all information required by the form, including security clearance data. There may be instances when clearance data is not known or available in the originating office. Under these conditions the Security Office should be contacted to obtain the necessary information. If the urgency does not allow sufficient time for normal processing of the visit request, a naval message may be sent. The message should contain essentially the same information as provided by Exhibit 2-11 and in all cases, cite SPAWAR Communications Standard Subject Identification Code (SSIC) 5500. Under extreme emergencies cognizant security coordinators are to telephone/telecopy security clearances to the activity being visited. It should be noted that some activities do not accept telephone certifications. Under no circumstances will visitors handcarry their own visit request.

b. Distribution of OPNAV Form 5521/27. Distribution will be made by the originating office as follows:

(1) Original and one copy to the addressee.

(2) One copy to the cognizant Security Coordinator.

(3) One copy to be retained by the originating office.

(4) In case of contractors, one copy to contractor's supporting Director of Industrial Security.

c. Termination of Visit Authorization. When an employee's status changes, i.e., reassignment, separation, termination of security clearance, or any other factor which eliminates the need to visit, the originating office shall immediately notify all activities holding valid visit requests that the individual's visit authorization is cancelled.

d. Security Coordinators. Security Coordinators shall monitor visit notifications released by their respective areas of cognizance for proper compliance with this Chapter and handle emergency outgoing telephone clearance notifications.

e. Disclosure Limitations. All disclosure of classified information shall be limited to the extent necessary to accomplish the purpose of the visit and shall not exceed the security clearance eligibility or "need-to-know" of the recipient.

f. Delegation of Authority. Personnel authorized to sign/release official correspondence are authorized to certify clearance data of their employees and/or sponsored personnel as required for advance visit notifications. The only exception to this delegation is that the signing official may not certify his own clearance. In this regard, Deputy Commanders and equivalent may designate qualified members of their staff to certify security clearances. The Security Office will certify clearances for Deputy Commanders or their equivalent as necessary. SPAWAR 00E/00A are authorized to certify clearances for SPAWAR 00/09.

2. Visits abroad not involving official contact with foreign nationals are subject to the provisions of OPNAVINST 4650.11 (current series). Visits abroad requiring official contact with foreign nationals are subject to the provisions of Chapter 6.

0248. UNAUTHORIZED VISITORS

SPAWAR personnel shall notify the Security Office immediately of any visitor who has no authorized building pass, whose identity cannot be satisfactorily established or whose presence in SPAWAR spaces is not authorized or desired.

0249. AREA CONTROL

1. Those areas within SPAWAR in which extensive or unusually sensitive classified matter or technical information are held or discussed, and where the occupant feels that adequate security cannot be maintained, shall be brought to the attention of the Security Office (SPAWAR 10H3). When necessary, additional protection and controls will be established. SPAWAR offices are encouraged to evaluate control measures in sensitive areas, such as location of mail desks, accessibility to conference rooms, and display rooms. The following factors should be considered in evaluating the security requirements of such areas:

2. Locate mail desks, computer terminals, personal computers, and printers in such a manner that unauthorized persons will not have deliberate or casual access to classified matter or material being processed. Provide continuous watch when material is exposed.

3. Establish internal visitor control procedures for access to classified display areas. Verify "need-to-know" and clearance of all visitors to the area, and maintain visit records to include name of visitor, company/activity represented and date and times of visit. Maintain continuous surveillance when classified material is exposed.

0253. DISCIPLINARY ACTION

1. Determination of appropriate disciplinary action is primarily a supervisor's responsibility. The object of discipline is to correct offenders and maintain discipline and morale among all personnel. Supervisors shall impose the minimum penalty that can reasonably be expected to achieve these objectives. Therefore, unless factors such as willful disregard, gross negligence, a pattern of poor security conduct or other extenuating circumstances exist, informal discipline should be the primary consideration. As a Command policy informal discipline will be in the form of a letter of caution for civilian and a non-punitive letter of caution for military personnel. Informal discipline is not made a matter of record in the individual's personnel folder. Supervisors shall consider administering formal discipline when a second infraction is committed within a one (1) year period from the date of the last infraction.

a. Civilian

Disciplinary actions for civilian-employees include Letters of Reprimand, Suspension and Removal from Federal Service. Prior to initiating disciplinary action for civilian employees, supervisors should seek guidance from SPAWAR 18.

b. Military

(1) See Manual for Courts-Martial.

c. Factors. To aid supervisors in arriving at an equitable decision to recommending penalties, the following are factors to be considered:

(1) The classification and volume of the jeopardized material.

(2) Consideration of the past record of the individual in terms of proven reliability, dedication to work, trustworthiness, etc.

(3) Previous record of security violations.

(4) Any extenuating circumstances under which the violation occurred.

(5) The adequacy of security guidance provided or available.

(6) If the violation was a result of willful disregard of security regulations.

Section 13

MEETINGS, CONFERENCES, AND SYMPOSIA

0254. GENERAL

The Chief of Naval Operations establishes Navy Department policy regarding classified disclosures through meetings and elaborates on the need to develop sound security practices in connection therewith. The fundamental security principle employed by the Department of Defense is based on the premise of circulation control, i.e., the control of the dissemination of classified information. Therefore, knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national security and only if they have been determined to be trustworthy. Responsibility for establishing the necessary safeguards to ensure compliance with this principle is sometimes overlooked or not clearly defined when meetings are involved. This is especially true when the meetings involve attendance/participation by large groups consisting of a variety of military agencies and industrial concerns. It is the intent of this section to clarify responsibilities and, thereby, assure that all security requirements are satisfied prior to SPAWAR sponsoring or presenting classified information at meetings.

0255. RESPONSIBILITY FOR CLASSIFIED MEETINGS HELD AT SPAWAR HEADQUARTERS

1. The term "meetings" applies to those situations where classified information is disclosed at formal presentations. It does not apply to the day-to-day meetings with other military personnel and contractors when the clearance and "need-to-know" factors have previously been established and are clearly apparent and when such meetings will be accomplished within assigned office space under normal area controls in accordance with paragraph 0249.2 of this Chapter.

2. SPAWAR Management Information Center (MIC). Security of meetings held in the MIC (Rooms 2E78 and 9W67) is the responsibility of the sponsor. Security of meetings sponsored by SPAWAR 00/09 is assigned to SPAWAR 18-55, who will be responsible for ensuring that all attendees possess adequate clearance for the classification of the meeting. SPAWAR 18-55 will monitor and schedule all usage of the MIC in order to preserve the physical security integrity of the MIC and to ensure that the sponsors of meetings are cognizant of the physical security requirements outlined by paragraph 0257. Sponsors of meetings held in Room 9W67 shall possess (at the minimum) a Secret security clearance due to the sensitivity of meetings held in this room. Sponsors will

be required to sign a Security Form (SPAWAR 5530/1) (Exhibit 2-13), which in essence states the sponsor has read and is cognizant of the security instructions pertaining to the use of the MIC, and that the sponsor is responsible for the physical security of the MIC Conference Room for the duration of the meeting and/or until such time as the responsibility for physical security of the MIC has been properly relinquished to SPAWAR 18-55 (copies of these forms will be provided to the Security Office for monitoring as necessary.) Meetings held in the MIC will normally be scheduled to adjourn before the close of SPAWAR working hours (1530). In the event that a meeting does continue beyond 1530 and/or in the absence of SPAWAR 18-55 personnel, the sponsor at the conclusion of the meeting will secure the MIC Conference Room and office in the presence of the SPAWAR Duty Officer.

3. Announcements of or invitations to attend classified meetings for prospective U. S. participants and attendees shall be sent only to organizations or persons that possess the necessary security clearance and have a validated need-to-know. The announcements or invitations will be sent by or on behalf of the SPAWAR official who authorizes the meeting. Foreign governments and their representatives and contractors may be invited after SPAWAR 10H determines that the applicable requirements of this instruction have been satisfied.

0256. RESPONSIBILITY FOR CLASSIFIED MEETINGS HELD OUTSIDE SPAWAR HEADQUARTERS

1. The Office of Naval Technology Transfer and Security Assistance (NAVOTTSA) or higher authority approves disclosure of classified information to foreign nationals. (Certain authority in this area has been delegated to SPAWAR by NAVOTTSA, see Chapter 6.)

2. The Chief of Naval Operations approves disclosure of classified information to personnel outside the executive branch of the Government. (Except when required in support of tasks or services essential to the fulfillment of a classified contract or approved program.)

3. Security Office. Because of the many security conditions that must be evaluated and satisfied, responsibility for coordinating classified disclosures as described above is assigned to the Security Office. In implementation of this responsibility, SPAWAR 10H will:

a. Obtain NAVOTTSA approval, when required.

b. Ensure that the physical security requirements outlined by paragraph 0257 and all other security requirements have been or will be satisfied.

c. Provide security guidance and direction as required.

d. Arrange for technical countermeasure surveys (to detect clandestine listening devices) when considered necessary.

4. Sponsor/Participants. Shall ensure that Security Office approval is obtained prior to disclosing or authorizing classified disclosures. In order to provide the basis for evaluating the security factors involved, the Security Office requires the following information at least 30 days prior to the meeting: (Exceptions to the 30-day requirement will be granted when extenuating circumstances exist, such as for bidders conference when procurement lead time is a factor.)

a. The proposed date(s) and the specific location of the meeting.

b. The identification of attendees and the basis for their need to attend.

c. The specific purpose of the meeting as relates to the Command's mission and the identification and classification of the information to be presented.

d. The name(s) of the individual(s) who will be responsible for ensuring that the physical security requirements outlined by paragraph 0257 below are complied with.

0257. PHYSICAL SECURITY REQUIREMENTS

When sponsoring a meeting, the sponsoring office is responsible for the following minimum security measures:

1. Conducting a thorough inspection of the conference room, auditorium, etc., prior to each meeting or session to remove unauthorized persons, packages, briefcases, etc.

2. Security monitoring for the duration of the meeting to prevent unauthorized access.

3. Positive identification and admittance of only authorized attendees, i.e., those with proper personnel security clearance and valid need for access.

4. Maintaining records of attendance.

5. Providing for the storage of classified material, when required.

6. Notifying attendees of the specific classification of all presentations.

7. Prohibiting the taking of classified notes. (Unless specifically authorized and proper accountability controls established.)

8. Ensuring that classified transcripts, related documents, etc., are not indiscriminately disseminated. All classified documentary information to be taken out of the custody of the Command shall be transmitted officially in accordance with the established correspondence procedures. All Secret material will be processed through SPAWAR 18-512.

9. Immediately at the close of a meeting, a security tour of the spaces utilized shall be made to ensure that classified papers, films, slides, etc., are not left adrift.

Section 14

NON-SPAWAR PERSONNEL ASSIGNED TO SPAWAR

0258. DEFINITION

Non-SPAWAR personnel are defined as those persons working full-time in SPAWAR Headquarters spaces who are not assigned to SPAWAR Headquarters for civilian payroll or personnel control purposes, ceiling control or military administration, or Temporary Additional Duty (TAD). These non-SPAWAR personnel are employees of other U. S. Government agencies, industrial contractors, representatives of foreign governments, or other individuals authorized to perform tasks in conjunction with SPAWAR programs, projects or contracts. Officers assigned as Liaison Officers and officers assigned on special projects are considered as SPAWAR employees.

0259. IDENTIFICATION AND AUTHORITY

Non-SPAWAR personnel will not be identified, specifically or by implication, either orally or in writing, as being an integral part of an official SPAWAR office designation, nor will they be listed in official DoD publications unless the individual's parent organization is clearly identified. Non-SPAWAR personnel will not sign SPAWAR correspondence, route sheets or other official documents.

0260. ACTION

1. The SPAWAR Division Head and/or Project Manager having primary technical cognizance over the work to be performed by non-SPAWAR personnel will assume sponsorship of such personnel and ensure that the following procedures are adhered to immediately upon arrival of the non-SPAWAR employee:

a. Security Arrangement. The person being sponsored shall complete the Non-SPAWAR Employee Data Card and Security Agreement (SPAWAR Form 5512/8) (Exhibit 2-14), in duplicate. This form will be witnessed by the head of the sponsoring office or an individual designated by him to perform this function. The original, with a copy of the individual's security clearance certification, assignment authorization, and access limitations notice (b below) will be forwarded to the Security Office. The duplicate form will be retained by the sponsoring office. SPAWAR Form 5512/8 is stocked in the Security Office.

b. Access Limitations. Access limitations will be established for each non-SPAWAR individual assigned. These limitations will conform with the provisions and intent of both the Navy and SPAWAR Security Manuals and may include other restrictions deemed to be necessary in the interest of the Command. Limitations imposed by the sponsoring code will vary depending upon the purpose of assignment, security clearance, parent organization, etc., and may include instructions on access to specific areas within the Headquarters as well as to classified or other sensitive information. In each case, the individual will be notified by his sponsoring code, in writing, of limitations imposed and required to acknowledge, by signature, the receipt of such notification. A copy of this access limitation notice will be retained by the sponsoring office and updated, as necessary, to conform to any changes in working requirements. One copy of the access limitations notice, and any subsequent changes thereto, will be forwarded to the Security Office.

c. Access Controls. All SPAWAR employees having a close working relationship with non-SPAWAR personnel must be made aware of the requirement for maintaining a continual vigilance to preclude the unauthorized disclosure of classified material as well as contractual, procurement, proprietary or other sensitive categories of information regardless of classification, the release of which is prohibited or would be prejudical to the interest of the Department of the Navy. The sponsoring office will establish internal access controls which will include, as a minimum:

(1) The assignment of non-SPAWAR personnel to working space which will be conducive to averting unauthorized disclosures by visual observation or audio interception;

(2) Stringent rules governing the receipt, processing, distribution, and storage of sensitive correspondence and documents; and

(3) Continual surveillance by SPAWAR employees over material work areas, and storage containers to which access by non-SPAWAR personnel is not authorized.

2. The Security Office will:

a. Assist the designated sponsoring office, as required, in complying with the requirements of this directive.

b. Provide additional security guidance as may be required on a case-by-case basis for non-SPAWAR individuals assigned to duty within SPAWAR.

c. Assist sponsoring office in establishing definitive guidelines on disclosure limitation to be imposed on non-SPAWAR personnel.

d. Conduct periodic reviews and inspections of security procedures effected by SPAWAR offices in compliance with this manual.

e. Issue building passes to employees upon receipt of SPAWAR Form 5512/8.

0261. REPORTING VIOLATIONS

Any violation of the foregoing procedures, failure of non-SPAWAR personnel to comply with instruction issued pursuant to the provisions of this instruction, or any action by such non-SPAWAR personnel which indicates an undue interest in information or other matters which they have not been authorized to receive or for which a clear "need-to-know" cannot be determined will be reported immediately to the Security Office.

Section 15

QUESTIONNAIRES

0262. DISCUSSION

From time to time SPAWAR employees receive questionnaires from industrial firms or their public relations representatives. The subject matter may vary from a routine reader habits inquiry to a complex evaluation of industrial capabilities or precise questions pertaining to Command organization, staffing, funding and technical requirements. It is an established fact that, despite the expressed intent or apparent innocence of such inquiries, it is possible through controlled and selective distribution to develop an informed and authoritative evaluation of major U. S. industrial capabilities or potential.

Other types of inquiries develop information concerning Government agencies which can pinpoint areas of primary effort and changes in emphasis resulting from high level policy decisions. In the hands of unfriendly foreign Governments such information could influence future intelligence collection and evaluation efforts.

0263. POLICY

Most industrial questionnaires addressed to SPAWAR employees pertain to official information. Due to the possibility of subversive intent inherent in every industrial questionnaire and the lack of any advantage to the Navy Department, a policy of "no reply" has been adopted. This policy does not apply to inquiries from other government agencies or from industrial firms clearly sponsored by them.

0264. ACTION

SPAWAR Headquarters employees who receive questionnaires, in any form, regardless of the method of receipt, that pertain to their position or duties shall make no reply. All material received shall be fowarded to the Security Office for review and referral to the Naval Investigative Service Command (NISCOM), when appropriate.

Section 16

COMMUNIST PROPAGANDA

0265. ACTION

1. Headquarters Personnel. SPAWAR personnel receiving such propaganda material, or suspected propaganda material, will transmit it to the Security Office for forwarding to the Naval Investigative Service Command (NISCOM) Headquarters. A brief report of the circumstances involved will be included when transmitting material to the Security Office.

2. SPAWAR Activities Personnel. Field Activity personnel receiving such material will forward it to their Security Manager who will transmit it to the nearest Naval Investigative Service Command (NISCOM) Office serving their area. A brief report of the circumstances involved will be included when transmitting material to the Naval Investigative Service Command (NISCOM) Office. Copy of all transmittals will be furnished to the SPAWAR Security Office.

Section 17

LIAISON WITH INVESTIGATIVE AGENCIES

In all matters pertaining to processing personnel security investigations, or other investigations, the Security Office will maintain official liaison with the Office of Personnel Management and the Defense Investigative Service (DIS). The Security Office will also maintain official liaison with the Naval Investigative Service Command (NISCOM) Headquarters, the FBI, and other law enforcement and investigative agencies. All inquiries and visits by representatives of law enforcement or investigative agencies shall be referred to the Security Office prior to making any disclosures.

Section 18

UNAUTHORIZED ABSENTEES

When an individual (military or civilian) having access to classified material is on unauthorized absence, the individual's supervisor shall make an inquiry to determine the reason for the individual's absence, and if the individual's pattern of behavior may be inimical to the interests of national security, or there is evidence of foul play. The supervisor shall immediately furnish all details to the Security Office.

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

20 DEC 1988

IN REPLY REFER TO:

EXHIBIT 2-1

From: Commander, Space and Naval Warfare Systems Command
To:

Subj: AUTHORIZATION TO TRANSPORT CLASSIFIED MATERIAL INSIDE CONUS

Ref: (a) SPAWARINST 5510.3

1. In accordance with Article 0210 of reference (a), you are authorized to hand carry the following classified material.

a. From this Command: _____

_____

_____

_____

_____

Addressee: (Not required if material is to be returned to SPAWARSYSCOM within same day) _____

_____

_____

b. To this Command: (To be indicated only when a SPAWAR employee believes he may be returning to Headquarters with classified material.) This authorization is for courier purposes only. The decision to release classified material and the responsibility to prepare classified materials for transmission rest with the Agency processing the material, not with the courier.

2. The need for this authorization has been carefully considered and evaluated and the following certifications made:

a. This hand carry is in direct support and benefit to COMSPAWARSYSCOM.

b. Use of normal mail transmission channels would not permit delivery in time to meet COMSPAWARSYSCOM objectives.

c. This authorization does not authorize the use of commercial aircraft.

3. You will observe the following precautions while hand carrying this material:

a. A list of all classified material carried shall be prepared and maintained by your SPAWAR code, and all such material shall be accounted for upon your return.

Subj: AUTHORIZATION TO TRANSPORT CLASSIFIED MATERIAL INSIDE CONUS

b. You shall familiarize yourself with the procedures and requirements of reference (a), paragraph 0210, before hand carrying classified material under this authorization.

4. This authorization expires on the same day as issued.

By direction

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

20 DEC 1988
IN REPLY REFER TO:

EXHIBIT 2-2

From: Commander, Space and Naval Warfare Systems Command
To: Airport Manager

Subj: AUTHORIZATION TO CARRY CLASSIFICATION INFORMATION ABOARD COMMERCIAL PASSENGER AIRCRAFT

1. This is to certify that the individual identified herein has been designated an official courier of the Command and is authorized to carry the package containing classified material described below while traveling aboard
TRANS AM Flight 007 Date

Name John Doe SSN 123-45-6789

DOB 21 APR 37 HEIGHT 5'10" WEIGHT 180

Signature of Courier

Type of Identification: Department of Defense Building Pass 1-123455

Description of Package Material:

Item No.	Measurement	Addressee	Addressor
1	8" X 10" X 10"	NAS	SPAWAR
2	8" X 10" X 10"	NAS	SPAWAR

Point of Departure: National Airport, Washington, DC

Destination: San Diego, CA

Transfer Points: None

2. Verification of this authorization may be made by calling the undersigned Security Officer of the Space and Naval Warfare Systems Command during duty hours (0700-1600) on (202) 692-8667 or the Command Duty Officer at all other times including weekends and holidays on (202) 692-8959.

3. This authorization is effective on date of this correspondence and expires on _____.

G. L. HARDGROVE
By direction

Copy to:
Command Duty Officer

20 DEC 1988

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

IN REPLY REFER TO:

5510
Ser 10H/

EXHIBIT 2-3

From: Commander, Space and Naval Warfare Systems Command
To:

Subj: APPOINTMENT OF SECURITY COORDINATOR

Ref: (a) SPAWARINST 5510.3H

1. You are appointed Security Coordinator for

2. In carrying out the responsibilities of this appointment, you shall thoroughly familiarize yourself with the duties outlined by paragraph 0230 of reference (a).

3. Upon receipt of this letter, you will contact the SPAWAR Security Office, Room 1S11 of National Center One (NC-1), to schedule an orientation briefing. Phone 692-8651/8667 to schedule your orientation briefing.

G. L. HARDGROVE
By direction

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

20 DEC 1988

IN REPLY REFER TO:

Date

EXHIBIT 2-4

MEMORANDUM

From:
To: SPAWAR 10H
Via: Deputy Commander, Program Director or Equivalent

Subj: SECURITY COORDINATOR INSPECTION REPORT

Encl: (1) Security Coordinator Inspection Report

1. The inspection required by paragraph 0230.2b has been completed. The results are reported on enclosure (1).

2. This report covers the following SPAWAR offices:

_____
SECURITY COORDINATOR

SECURITY COORDINATOR INSPECTION REPORT

A. Requirement. General office practice provides for verification of security clearance and official need for all visitors. Visitors are immediately challenged and identified upon entering office areas.

Remarks:

B. Requirement. New personnel are oriented in office and Command security practices on arrival or initial assignment to their office.

Remarks:

C. Requirement. There is a formal double check system (using SF 701) at the close of business that will ensure that all material is properly secured and each security container checked, etc.

Remarks:

D. Requirement. Safe and padlock combinations are changed when there is a transfer of personnel and at least every 12 months. (Containers with NATO and COMSEC material shall be changed every six months.)

Remarks:

E. Requirement. Only approved security containers are used for storage of classified material and such containers are in good mechanical condition.

Remarks:

F. Requirement. All Secret material is being accounted for. Any unrecorded Secret documents must be taken to SPAWAR 18-512 for official recording.

Remarks:

G. Requirement. All non-SPAWAR personnel assigned to SPAWAR office spaces are reported (SPAWAR 5512/8) and access controlled in accordance with the provisions of this manual.

Remarks:

H. Requirement. All foreign nationals visiting the Command are approved by the Security Office, in accordance with provisions of Chapter 6.

Remarks:

I. Requirement. A system for returning Secret documents to SPAWAR 18-512 when no longer required is in operation and given continuous attention.

Remarks:

J. Requirement. Combinations to security containers shall be memorized. The only authorized written record is that which is maintained by the Security Office. (Offices having large numbers of containers may record combinations thereto, provided such records are protected to the same degree as the classified material involved.)

Remarks

K. Requirement. All Secret material being transmitted out of the Command, by mail or by hand, is processed through SPAWAR 18-512.

Remarks:

L. Requirement. Typewriter ribbons used in preparation of classified material are given the same classification and safeguards the same as the classified material typed. (Note: An exception to this requirement is granted for typewriter ribbons described in paragraph 0227.8 of.)

Remarks:

M. Requirement. Classification guidance for programs, contracts, task assignments, etc., has been issued and is reviewed on a regular basis to determine adequacy (Chapter 5.)

Remarks:

N. Requirement. Personnel responsible for preparation of contract security classification specification (DD Form 254) are thoroughly familiar with the requirements and guidance outlined by Chapter 3, SPAWARINST 5510.).

Remarks:

O. Requirement. All personnel are aware of and observe the prohibition against taking classified material to their residence for overnight storage.

Remarks:

P. Requirement. Security containers are not used for safeguarding personal property, especially valuable items.

Remarks:

Q. Requirement. Commercial aircraft is not used when handcarrying classified material without required approval.

Remarks:

R. Requirement. Classified information is not released to foreign nationals or governments without approval from the Security Office (Chapter 6)

Remarks:

S. Requirement. Intelligence information is not released to industry without approval from the Security Office.

Remarks:

T. Requirement. Sponsors and participants in classified meetings are familiar with the requirements of Section 13, Chapter 2, .

Remarks:

U. Requirement. Supervisors are familiar with the factors/conditions which may be cause to withhold access to classified matter (Chapter 4)

Remarks:

V. Requirement. Secret material is not to be reproduced without prior approval of SPAWAR 18-51.

Remarks:

EXHIBIT 2-5

NOTE: This certificate due back to Security Office by_____

SECURITY ORIENTATION CERTIFICATE

I, _____, certify that I have read
(Name of Employee)
and understand the provisions of the SPAWAR Security Manual (SPAWARINST 5510.3) and the hand-out entitled "Custodial Security Requirements" and understand my responsibilities for safeguarding classified defense information entrusted to me.

_____ (Date)

_____ (Employee Signature)

_____ (Date)

_____ (Signature of Witness)
(Supervisor or Security Coordinator)

20 DEC 1988

Exhibit 2-6

General Services Administration

Rules and regulations governing public buildings and grounds

Federal Property Management Regulations 41 CFR 101-20.3

1. AUTHORITY. These rules and regulations are promulgated pursuant to Public Law 566, 80th Congress, approved June 1, 1948 (40 U.S.C. 318), and the Federal Property and Administrative Services Act of 1949 (63 Stat. 377), as amended.

2. APPLICABILITY. These rules and regulations apply to all property under the *charge and control of the General Services Administration and to all persons* entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations.

3. INSPECTION. Packages, briefcases, and other containers brought into, while on, or being removed from the property are subject to inspection. A full search of a person may accompany an arrest.

4. ADMISSION TO PROPERTY. Property shall be closed to the public during other than normal work hours. The closing of property will not apply to that space and in those instances where the Government has approved the after normal working hour use of building or other property space for commercial, cultural, educational, and recreational activities as authorized by the Cooperative Use Act of 1978 (Pub. L. 94-541). During normal work hours, property shall be closed to the public only when situations require such action to ensure the orderly conduct of Government business. The decision to close the property shall be made by the designated official under the Facility Self-Protection Plan after consultation with the buildings manager and the ranking representative of the Federal Protective Service responsible for protection of the facility or the area. This requirement does not preempt the authority of the Regional Director, Federal Protective Service Division, or any other authorized GSA official to affect a security alert at a facility. Any such action shall be coordinated with the designated official. The designated official is the highest ranking official of the primary occupant agency or an alternate high ranking official designated in advance by agreement of occupant agency officials. *When property is closed to the public, admission to such property will be* restricted to authorized persons who shall sign the building register and display Government or other identifying credentials when requested to do so by Federal Protective Officers or other authorized individuals. Entry upon property in violation of any of the above applicable provisions is prohibited.

5. PRESERVATION OF PROPERTY. The improper disposal of rubbish on property, the willful destruction of or damage to property, the theft of property, the creation of any hazard on property to persons or things, the throwing of articles of any kind from or at a building, or the climbing upon statues, roof, or any part of the building, is prohibited.

6. CONFORMITY WITH SIGNS AND DIRECTIONS. Persons in and on property shall at all times comply with official signs of a prohibitory, regulatory, or directory nature and with the direction of Federal Protective Officers and other authorized individuals.

7. DISTURBANCES. Any unwarranted loitering, disorderly conduct, or other conduct on property which creates loud or unusual noise or a nuisance, which unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots, which otherwise impedes or disrupts the performance of official duties by Government employees, or which prevents the general public from obtaining the administrative services provided on the property in a timely manner, is prohibited.

8. GAMBLING. Participating in games for money or other personal property or *the operating of gambling devices, the conduct of a lottery or pool, or the* selling or purchasing of numbers tickets, in or on property is prohibited. This prohibition shall not apply to the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a State law and conducted by an agency of a State as authorized by section 2(a)(5) of the Randolph-Sheppard Act (20 U.S.C. 107 et seq.).

9. ALCOHOLIC BEVERAGES AND NARCOTICS. Operating a motor vehicle while on the property by a person under the influence of alcoholic beverages, narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines, is prohibited. Entering upon the property, or while on the property, under the influence of, or using or possessing any narcotic drug, hallucinogen, marijuana, barbiturate, or amphetamine is prohibited. This prohibition shall not apply in cases where the drug is being used as prescribed for a patient by a physician. Entering upon the property, or being on the property, under the influence of alcoholic beverages is prohibited. The use of alcoholic beverages on property is prohibited except upon occasions and on property upon which the Administrator of General Services or the Regional Administrator of the General Services Administration has for appropriate official uses granted an exemption in writing.

10. SOLICITING, VENDING, AND DEBT COLLECTION. Soliciting alms and contributions, commercial soliciting and vending of all kinds, displaying or distributing commercial advertising, or collecting private debts in or on GSA-*controlled property is prohibited. This rule does not apply to (a) national or* local drives for funds for welfare, health, or other purposes as authorized by the "Manual on Fund Raising Within the Federal Service" issued by the U.S. Civil Service Commission under Executive Order 10927 of March 18, 1961, and sponsored or approved by the occupant agencies, (b) concessions or personal notices posted by employees on authorized bulletin boards, and (c) the distribution of labor organization membership or dues authorized by occupant agencies under Executive Order 11491 of October 29, 1969, as amended.

DISTRIBUTION OF HANDBILLS. Posting or affixing materials such as pamphlets, handbills, or flyers on bulletin boards or elsewhere on property is prohibited, except as authorized in § 101-20.308 or when such displays are conducted as part of authorized Government activities. Distribution of materials such as pamphlets, handbills, or flyers is prohibited, except in those areas of the property open to the public such as entrances, lobbies, and open corridors, unless conducted as part of authorized Government activities. The buildings manager or his representative shall be advised in advance of the proposed distribution in public areas, but he shall not exercise control over the content of the material.

12. PHOTOGRAPHS FOR NEWS, ADVERTISING, OR COMMERCIAL PURPOSES. Photographs may be taken in space occupied by a tenant agency only with the consent of the occupying agency concerned. Except where security regulations apply or a Federal court order or rule prohibits it, photographs for news purposes may be taken in entrances, lobbies, foyers, corridors, or auditoriums when used for public meetings. Subject to the foregoing prohibitions, photographs for advertising and commercial purposes may be taken only with written permission of an authorized official of the agency occupying the space where the photographs are to be taken.

13. DOGS AND OTHER ANIMALS. Dogs and other animals, except seeing eye dogs or other guide dogs, shall not be brought upon property for other than *official purposes.*

14. VEHICULAR AND PEDESTRIAN TRAFFIC. (a) Drivers of all vehicles entering or while on property shall drive in a careful and safe manner at all times and shall comply with the signals and directions of Federal Protective Officers or other authorized individuals and all posted traffic signs. (b) The blocking of entrances, driveways, walks, loading platforms, or fire hydrants on property is prohibited, and (c) Except in emergencies, parking on property is not allowed without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation, where warning signs are posted, shall be subject to removal at the owners risk and expense. This paragraph may be supplemented from time to time with the approval of the Regional Administrator by the issuance and posting of such specific traffic directives as may be required, and when so issued and posted such directives shall have the same force and effect as if made a part hereof. Proof that a motor vehicle was parked in violation of these regulations or directives may be taken as prima facie evidence that the registered owner was responsible for the violation.

15. WEAPONS AND EXPLOSIVES. No person entering or while on property shall carry or possess firearms, other dangerous or deadly weapons, explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes.

16. *NONDISCRIMINATION. There shall be no discrimination by segregation or* otherwise against any person or persons because of race, creed, sex, color, or national origin in furnishing or by refusing to furnish to such person or persons the use of any facility of a public nature, including all services, privileges, accommodations, and activities provided thereby on the property.

17. PENALTIES AND OTHER LAWS. Whoever shall be found guilty of violating any rule or regulation in this Subpart 101-20.3 while on any property under the charge and control of GSA is subject to a fine of not more than $50 or imprisonment of not more than 30 days, or both. (See 40 U.S.C. 318c.) Nothing in these rules and regulations shall be construed to abrogate any other Federal laws or regulations or any State and local laws and regulations applicable to any area in which the property is situated. (Sec. 205(c), 63 Stat. 390, 40 U.S.C. 486(c)).

Jay Solomon

Jay Solomon

Administrator of General Services

July 5, 1978

EXHIBIT 2-7

20 DEC 1988

REPORT OF LOSS OR THEFT

CHECK ☐ LOSS ☐ THEFT

INSTRUCTIONS

This form should be completed by the person most familiar with the facts of the loss or theft. *(Please type or print.)* This person should check appropriate title block in upper right hand corner and complete sections I, II and III-1.

NUMBER COPIES AND DISTRIBUTION.

LOSS - Complete one copy - To be retained by the GSA Police Office or other designated location.

THEFT - Government Property or Personal ITEMS - Complete original and three copies to be distributed as follows:
- Original and two copies - Regional GSA Federal Protective Service Division
- One copy - GSA Buildings Manager or GSA FPO Supervisor

NOTE: The GSA Police Office or Buildings Manager will complete section III-2 and 3, as appropriate, prior to forwarding.

I. PERSON REPORTING LOSS OR THEFT

NAME | OFFICE TELEPHONE NO. | EXTENSION

DEPARTMENT | OFFICE ADDRESS *(Include room no. and building)* | STREET, CITY, STATE AND ZIP CODE

DATE OF LOSS OR THEFT | TIME | PLACE

II. DESCRIPTION OF PROPERTY LOST OR STOLEN

NAME OF ARTICLE | OWNERSHIP ☐ GOVT ☐ PERSONAL | ESTIMATED VALUE $

DESCRIPTION *(Include serial numbers, identifying marks, make, model, color, size, condition, etc.)*

DETAILS OF LOSS OR THEFT *(Include information as to how loss or theft discovered and information as to suspects, witnesses and recovery of property.)*

(If more space is needed, attach additional sheet(s).)

SIGNATURE OF PERSON REPORTING LOSS | TELEPHONE NO. | DATE SIGNED

III. ACTION TAKEN BY

1. COMPLAINANT — IF PERSONAL PROPERTY, WAS THE LOCAL POLICE DEPARTMENT NOTIFIED? ☐ YES ☐ NO *(If "Yes," identify the person notified.)*

TO BE COMPLETED BY GSA OFFICIALS ONLY

2. FPO OFFICE — DATE AND TIME GSA FORM 182 RECEIVED | PERSON NOTIFIED | DATE AND TIME NOTIFIED

ACTION TAKEN *(Arrests, preliminary investigations, recoveries, etc.)*

3. BLDG. MGR. OR FPO SUPERVISOR — DATE AND TIME GSA FORM 182 RECEIVED | PERSON NOTIFIED | DATE AND TIME NOTIFIED

4. FEDERAL PROTECTIVE SERVICE DIVISION — DATE AND TIME GSA FORM 182 RECEIVED | WAS FBI NOTIFIED? ☐ YES ☐ NO | IF "YES," NAME OF PERSON

WAS LOCAL POLICE DEPARTMENT NOTIFIED BY YOU? ☐ YES ☐ NO *(If "Yes," identify)*

[illegible]

20 DEC 1988

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

IN REPLY REFER TO:

Date

EXHIBIT 2-8

MEMORANDUM

From:
To: SPAWAR 10H

Subj: REQUEST FOR DOD BUILDING PASS FOR CONTRACTOR EMPLOYEE

Ref: (a)

Encl: (1) Copy of current Visit Request

1. In accordance with reference (a), enclosure (1) is forwarded with a request that the individual(s) listed be issued a DoD Building Pass.

2. Access is required to the following building(s):

Building	Room No.	Point of Contact and Telephone Number

3. Unescorted access to the above building(s) is required for performance of the following specific tasks under Contract No._____.

_____
Must be signed by Directorate Head,
Program Director or equivalent.
(By direction signature not acceptable)

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

20 DEC 1989

IN REPLY REFER TO:

Date

EXHIBIT 2-9

From: _____ SPAWAR_____
EMPLOYEE NAME CODE

To: Security Office (SPAWAR 10H)

Via: _____
EMPLOYEE'S SUPERVISOR

Subj: REPORT OF LOST OR STOLEN BUILDING PASS

Ref: (a) SPAWARINST 5510.1
(b) SPAWARINST 5530.1

1. In accordance with references (a) and (b), I am reporting the loss of my building pass.

_____
TYPE OF PASS (DOD (NCR OR TEMPORARY)), GSA 15, ETC.)

_____
DATE LOST (BEST GUESS)

2. The circumstances surrounding this loss are as follow: (Indicate area where you think loss occurred, or if you think it was stolen, why. Tell what efforts you have made to find the missing building pass.

3. I have/have not lost a building pass previously.

_____ _____
(SUPERVISORS SIGNATURE) (EMPLOYEE SIGNATURE)

ACTION TAKEN BY SECURITY OFFICE:
New DoD badge issued: _____ _____
TYPE OF BADGE EXPIRATION DATE

_____
NEW BADGE NUMBER (IF ANY)

EXHIBIT 2-10

20 DEC 1988

ROUTE SLIP AND OFFICE MEMO
SPAWAR 5216/1 (Rev. 9-85)

DO NOT DETACH FROM OFFICIAL CORRESPONDENCE.
WRITE OR PRINT LEGIBLY IN INK.

CONTROL NO.	REPLY DUE BY

ORIGINATOR *(Code, and Extension when applicable)*	SERIAL	DATE	SUBJECT CLASS	CROSS REF.
SPAWAR VISITOR CONTROL OFFICE			UNCLAS	

SUBJECT: VISIT REQUESTS

ENCLOSURE

ROUTE TO CODE	SYMBOL	RELEASED INITIAL	DATE MON.	DAY	YEAR	SIGNATURE, EXT. CODE AND DATE ARE TO FOLLOW COMMENTS SYMBOLS: A- Action C - Comment I - Information P - Prepare Reply R - Retain Copy
SPAWAR/PMW						1. THE ATTACHED VISIT REQUEST HAS BEEN REVIEWED BY THE VISITOR CONTROL OFFICE. THE PERSONNEL LISTED ON THE VISIT REQUEST ARE ELIGIBLE TO RECEIVE CLASSIFIED INFORMATION THROUGH THE DEGREE OF CLEARANCE INDICATED. HOWEVER, CLASSIFIED DISCLOSURES ARE ONLY PERMITTED WHEN THE PROSPECTIVE RECIPIENT HAS A REQUIREMENT FOR ACCESS IN ORDER TO PERFORM TASKS ON SERVICES ESSENTIAL TO FULFILLING A CLASSIFIED SPAWAR CONTRACT OR PROGRAM OR WHEN PROPERLY JUSTIFIED UNDER OTHER FEDERAL GOVERNMENT AGENCY SPONSORSHIP. CLASSIFIED DISCLOSURES ARE NOT AUTHORIZED UNTIL THE FOREGOING CONDITIONS HAVE BEEN SATISFIED.
						2. IF THE VISIT REQUESTED IS NOT ACCEPTABLE, OR IF ADDITIONAL LIMITATIONS ARE REQUIRED, E.G., A DIFFERENT DATE, A SHORTER TIME PERIOD, ETC., RETURN THIS REQUEST AND ROUTE SHEET TO THE VISITOR CONTROL STATING YOUR LIMITATIONS.
						3. IF THIS VISIT IS ACCEPTABLE TO YOU, AS THE INDICATED POINT OF CONTACT, ADDITIONAL ACTION IS NOT REQUIRED. WHENEVER YOU RELEASE CLASSIFIED INFORMATION, HOWEVER, YOU ARE REQUIRED TO ASSURE YOURSELF THAT THE RECIPIENT CONTINUES TO HAVE A VALID NEED TO KNOW AND IS AUTHORIZED TO RECEIVE CLASSIFIED INFORMATION.

FILE	UNLESS THIS MATERIAL IS TO BE FURTHER ROUTED – RETURN TO FILE BY DATING AND INITIALING.	INITIAL	DATE

EXHIBIT 2-11

PRIVACY ACT STATEMENT ON REVERSE

20 DEC 1988

VISIT REQUEST

VISITOR CLEARANCE DATA

OPNAV 5521 27 (REV. 1-75) S/N 0107-LF-055-2235

(SEE CURRENT EDITION OF OPNAVINST. 5510.1 FOR DETAILED INSTRUCTIONS)

CHECK ONE

☐ REPLY REQUIRED

☐ REPLY ONLY IF NEGATIVE

FROM (COMPLETE ADDRESS OF REQUESTING ACTIVITY)	DATE OF REQUEST
	SPECIFIC PERSONNEL OR SECTION OF COMMAND TO BE VISITED

FOLD ON THIS LINE

DURATION OF VISIT (ARRIVE)	(DEPART)	DEGREE OF ACCESS REQUIRED

PURPOSE OF VISIT/REMARKS (IF THE VISIT IS TO A CONTRACTOR FACILITY, INCLUDE CONTRACT NUMBER IF APPROPRIATE)

NAME, RANK, TITLE OR POSITION, SOCIAL SECURITY NO.	DATE AND PLACE OF BIRTH	NATIONALITY (CHECK ONE)	LEVEL OF SECURITY CLEARANCE
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	
		U.S. CITIZEN	
		IMMIGRANT ALIEN	

NAME, RANK AND TITLE OF OFFICIAL AUTHORIZING VISIT AND CLEARANCE	SIGNATURE

COPY TO:

PRIVACY ACT STATEMENT

OPNAV 5521/27, Visit Request

AUTHORITY: E.O. 11652

PRINCIPAL PURPOSE: Information is obtained to identify personnel visiting activities when such visits are expected to involve access to classified information.

ROUTINE USE: Information provided in the form, when compared with information known to or normally in the possession of an individual, is used in determining whether or not an individual is who he purports to be when visiting an activity. The information may be disclosed to all those charged at the activity with making the foregoing determination.

DISCLOSURE: (Mandatory or voluntary; consequences, etc.): Completion of OPNAV 5521/27, including the disclosure of your Social Security Number, is voluntary. Failure on your part, however, to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers), may serve as a basis for denial of the request to visit, or for access to information classified in the national interest pursuant to E.O. 11652.

Exhibit 2-12

SCHEDULE OF FORMAL DISCIPLINARY ACTIONS
Range of Penalties for Stated Offenses
(Reprimands - Suspensions - Removal)

Nature of Offense	1st MIN - MAX	2nd MIN - MAX	3rd MIN - MAX
Failure to Safe-guard classified	Reprimand - 5 Days Suspension	5 Days - Suspension to Removal	10 Days - Suspension to Removal
When Classified Material has been Compromised	Reprimand - To Removal	5 Days - Suspension to Removal	10 Days - Suspension to Removal

20 DEC 1988

ACKNOWLEDGMENT CERTIFICATION OF SPAWAR PHYSICAL SECURITY RESPONSIBILITIES FOR SECURE CONFERENCE ROOMS

	9W67
	2E80

SPONSOR (PRINT NAME & CODE) _____

SUBJECT OF MEETING _____

CLASSIFICATION _____ DATE OF MEETING: _____ TIME (START/FINISH) _____

NOTE: THESE REQUIREMENTS APPLY WHETHER OR NOT THE MEETING IS CLASSIFIED.

I have read section 13 of the SPACE & NAVAL WARFARE SYSTEMS COMMAND SECURITY MANUAL and am cognizant of the security instructions that apply to meetings, specifically those covering the necessary security requirements found in paragraphs 0254 and 0255. As sponsor, I accept responsibility for the physical security of SPAWAR conference rooms [2E80, or the Management Information Center (M.I.C.), rm. 9W67] for the duration of the above meeting an/or until such time as the security responsibility for the conference room has been properly relinquished to SPAWAR 18-55 personnel. For room 2E80, this includes returning the key, after locking doors with it, immediately at close of meeting.

1. **Paragraph 0255 is herewith reprinted to insure that this portion concerning physical security requirements is clearly understood:**

PHYSICAL SECURITY REQUIREMENTS

WHEN SPONSORING A MEETING, THE SPONSORING OFFICE IS RESPONSIBLE FOR THE FOLLOWING MINIMUM SECURITY MEASURES:

- Conducting a thorough inspection of the conference room, auditorium, etc., prior to each meeting or session to remove unauthorized persons.
- Security monitoring for the duration of the meeting to prevent unauthorized access.
- Positive identification and admittance of only authorized attendees, (i.e., those with proper personnel security clearance and valid need for access.)
- Maintaining records of attendance.
- Providing for the storage of classified material, when required.
- Notifying attendees of the specific classification of all presentations.
- Prohibiting the taking of classified notes (unless specifically authorized and proper accountability controls established).
- Ensuring that classified transcripts, related documents, etc., are not indiscriminately disseminated. All classified documentary information to be taken out of the custody of the command shall be transmitted officially in accordance with the established correspondence procedures. All secret material will be processed through the command secret records custodian (SPAWAR 18-512).
- Immediately at the close of a meeting, a security tour of the spaces utilized shall be made to ensure that classified papers, films, slides, etc., are not left adrift.

2. **CAUTION: Non-compliance with the above requirements is a security violation and culpable individuals will be disciplined accordingly!**

SIGNED BY: (Sponsor) _____ (SPAWAR 10H) _____

3. **In the absence of SPAWAR 18-55 personnel, meetings adjourned after 1530 require that the sponsor secure the conference room in the presence of the SPAWAR Duty Officer.**

The SPAWAR MIC has been properly secured in accordance with paragraph 0254 and 0255 of the SPAWAR security manual. Signed by: (SPAWAR 18-55 Duty Officer) _____ Time/Date: _____

SPAWAR 5530/1(3/88)

EXHIBIT 2-14

20 DEC 1988

NAME (LAST, FIRST, INITIAL)		COMPANY/AGENCY REPRESENTED		SPONSORING CODE
SECURITY CLEARANCE	CLEARING AGENCY	COMPANY/AGENCY ADDRESS		
PROJECT/TASK/CONTRACT	DESCRIPTION OF WORK (UNCLASSIFIED)			DEGREE OF ACCESS REQUIRED
LOCATION IN SPAWAR	BEGINNING DATE	EXPIRES(MAXIMUM 12 MONTHS)	DATE OF SECURITY AGREEMENT	BUILDING PASS ☐ NO ☐ YES

REMARKS

SEE SECURITY AGREEMENT STATEMENT ON REVERSE SIDE

DATE DEPARTED _____

NON-SPAWAR EMPLOYEE DATA CARD AND SECURITY AGREEMENT SPAWAR 5512/8 (REV. 9-88)

(PREPARE IN DUPLICATE)

20 DEC 1988

EXHIBIT 2-15

ACTIVITY SECURITY CHECKLIST

ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
Irregularities discovered will be promptly reported to the designated Security Office for corrective action	Statement I have conducted a security inspection of this work area and checked all the items listed below.		

TO (If required) | FROM (If required) | THROUGH (If required)

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-103
NSN 7540-01-213-7900

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

20 DEC 1988

SECURITY CONTAINER CHECK SHEET

TO (if required)	THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

702-101
NSN 7540-01-213-7900

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

EXHIBIT 2-17

MEMORANDUM

From:
To: SPAWAR 10H

Subj: REQUEST FOR CARDKEY TO PERMIT ACCESS TO NC-1 PARKING GARAGE DURING NON-DUTY HOURS

1. It is requested that the following employee(s) be issued a cardkey for access to NC-1 parking garage during non-duty hours.

2. I certify that access is required at least once a week and the employee(s) has parking privileges.

3. The employee has been briefed that vehicles entering or leaving NC-1 are subject to inspection for contraband, unauthorized personnel or Government property.

_____
MUST BE SIGNED BY DIRECTORATE HEAD, PROGRAM DIRECTOR OR EQUIVALENT

EXHIBIT 2-18

5510
Ser 10H/

SAMPLE ONLY

From: Commander, Space and Naval Warfare Systems Command
To:

Subj: CLASSIFIED DOCUMENT DISTRIBUTION LIST

Ref: (a) OPNAVINST 5510.1

1. Paragraph 24-1 of reference (a) requires the Commander to limit access to SPAWAR originated material only to those who have a current "need-to-know."

2. On _____, you were provided _____ copy(s) of the following classified documents:

3. It has been determined, after a review by cognizant SPAWAR personnel, that you no longer require access to this material. The document(s) should be:

____ a. Returned to SPAWARSYSCOM, Attn:

____ b. Destroyed in the manner approved for this level of material. Provide a copy of the Certificate of Destruction to SPAWARSYSCOM, Attn:

_____
By direction

SAMPLE ONLY

CHAPTER III

INDUSTRIAL SECURITY AND DOMESTIC DISCLOSURES

Section 1

INDUSTRIAL SECURITY

0301. GENERAL

The security of the United States depends in part upon proper safeguarding of classified information released to industry. Contractors merely mark and protect information developed under a contract on the basis of a Contract Security Classification Specification (DD Form 254) which is issued by SPAWAR. SPAWAR is responsible for providing to contractors all security classification guidance necessary to properly classify information and material produced under the terms of the contracts. It is essential that comprehensive classification security guidance be furnished to SPAWAR contractors. Overall responsibility for administering the Industrial Security Program is assigned to the Defense Investigative Service, Director of Industrial Security.

0302. CLASSIFIED CONTRACTS

A classified contract is one which requires or will require access (including aural or visual) to classified information by the contractor or his employees in the performance of the contract. A contract may be classified even though the Contract Document (SF 26) itself or task is unclassified.

0303. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD Form 254)

1. The responsibility for preparing the DD Form 254 rests with the office having technical cognizance over the procurement. DD Forms 254 will be prepared using the format and entries shown in Exhibits 3-1 (RFP DD Form 254); 3-2 (Original Contract DD Form 254); 3-3 (Revised DD Form 254); and 3-4 (Final DD Form 254). The RFP, original, and revised DD Forms 254 will contain the most current classification guides (See para. 0521) available for the project, equipment or services being procured. The cognizant technical office is responsible for forwarding all classified guides, specifications, etc., to the contractor.

2. All DD Forms 254 shall be forwarded to the Contracting Officer for Security Matters (SPAWAR 10H) for review at the acquisition/procurement request stage. The Contracting Officer for Security Matters (SPAWAR 10H) will sign DD Forms 254 ONLY when a RFP or contract number and expiration date have been affixed. No entry changes will be made to a DD Form 254 after signature by the Contract- ing Officer for Security Matters.

3. Cognizant engineers will review the DD Form 254 biennially, as well as whenever classification guidance changes. Result of these reviews will be furnished to the Contracting Officer for Security Matters (SPAWAR 10H) who in turn informs the appropriate Director of Industrial Security and the contractor. Biennial reviews are not required for "access only" and service-type contracts where no classification guidance is required due to no generation of classified material.

4. When all classified aspects of a contract are completed, a final DD Form 254 (Exhibit 3-4) shall be prepared by the cognizant engineer and forwarded to the Contracting Officer for Security Matters (SPAWAR 10H) for review and signature. Final DD Forms 254 are not required when classified material accountability has been transferred to follow-on contracts via Item 6 of the follow-on contract DD Form 254.

5. The Contracting Officer for Security Matters (SPAWAR 10H) is responsible for coordinating all contractor requests for retention of classified informa- tion generated or received under a SPAWAR contract. Based upon the desires of the cognizant engineers, SPAWAR 10H will reply to the contractor, unless a final DD Form 254 is required.

0304. ITEM ENTRIES ON THE DD FORM 254

Items 1 through 14 and Item 16 provide the general administrative and contractual information pertaining to the classification specification of the classified effort. Item 15 and any supplement/attachments are used to provide the specified classification/downgrading/declassification information and/or Operations Security (OPSEC) considerations. Classified information will not be entered on the DD Form 254.

0305. VERIFICATIONS OF CLEARANCES

1. The Security Office will verify facility clearances relating to industrial security. Except where there is an existing contractual relationship between SPAWAR and the contractor involving classified material of the same or higher category, all actions resulting in the disclosure of classified information to a contractor will be cleared with the Security Office for verification of the contractor's facility clearance.

2. Facility security clearances verified by the Security Office are valid for a period of one year. Reconfirmation is not required as long as there is an existing contractual relationship involving classified information of the same or higher category.

0306. DISCLOSURES TO SPAWAR CONTRACTORS

1. Prior to the disclosure of any classified information to a SPAWAR contractor, the releasing SPAWAR office shall request the Security Office to determine that the contractor has a current facility clearance equal to or higher than the level of classified information to be disclosed. If the contractor will be required to have physical possession of classified material, the releasing SPAWAR office shall also request the Security Office to determine that the contractor has the ability to properly safeguard the classified information. In addition to determining clearances, the releasing office is responsible for determining "need-to-know."

2. Disclosures of intelligence information to SPAWAR contractors require the prior approval of the Security Office.

3. When Top Secret information is authorized to be released to Department of Defense contractors, such authorization shall include the following statements:

"This information is released under the condition that a record be kept by the recipient of all individuals who are afforded access to the information contained in the document, and that this record will be made available to the Department of Defense, if requested."

4. In addition, the office of issuance of the Top Secret document will be informed of the outside dissemination. The Security Office shall be advised of all Top Secret disclosures to industry, either by copy of letter of transmittal or other written form identifying the Top Secret information.

5. The responsibility to confirm the clearance of a contractor with the Security Office prior to award of a classified contract release material under a, RFP, RFQ, or IFB, rests with SPAWAR 12. Confirmation of a contractor's clearance prior to release of classified material under situations other than those indicated above, rests with the activity/individual releasing the material.

0307. TRANSMITTAL OF CLASSIFIED MATERIAL TO DOD CONTRACTORS

1. All classified material transmitted to a Department of Defense contractor shall be by one of the methods prescribed in paragraph 0214. Many contractors have more than one mailing address for unclassified correspondence; however, only one address is used to receive classified material. The sender of classified material must check with SPAWAR 10H for the

proper classified mailing address prior to shipment. There are five conditions which must be met before classified material may be transmitted to Department of Defense contractors.

2. The contractor must have an appropriate Department of Defense facility clearance.

3. The releasing SPAWAR office having cognizance over the contract or program under which classified material is being released must determine that the contractor has a "need-to-know."

4. A determination must be made that the recipient of the classified material has the ability to safeguard the material physically.

5. Classified material will only be furnished to a contractor on a letter of transmittal. One copy of the letter of transmittal will be furnished to SPAWAR 12-14.

6. SPAWAR offices releasing classified material directly to industrial representatives for hand delivery shall prepare and execute the certification memorandum for non-SPAWAR handcarries outlined by Exhibit 3-8. This memorandum will be hand delivered to SPAWAR 18-51 by the sponsoring office with the material to be hand delivered. If clearance data was not previously furnished to SPAWAR 18-51 by the sponsoring office, such information shall be verified with the Security Office.

Section 2

DISCLOSURES

0308. DISCLOSURES TO DEPARTMENT OF DEFENSE

SPAWAR personnel may release classified matter to other Department of Defense activities provided the activity meets the required "need-to-know", and all other applicable provisions of this manual are satisfied. SPAWAR offices releasing classified material directly to DoD representatives for hand delivery to Local Metropolitan Area Commands shall prepare and execute the certification memorandum for non-SPAWAR handcarries (Exhibit 3-8). This authorization will be hand delivered to SPAWAR 18-51 by the sponsoring office along with the material to be hand delivered. The sponsoring office must have the courier's clearance on file and furnish a copy to SPAWAR 18-51 or have it verified through the Security Office.

0309. DISCLOSURES TO NON-SPAWAR CONTRACTORS

Disclosure of classified information to appropriately cleared facilities engaged in classified contracts for Department of Defense (DoD) activities other than SPAWAR shall be approved by the Security Office. The DoD contracting activity must provide sufficient justification for such access on the part of their contractor to permit SPAWAR to establish the "need-to-know."

0310. DISCLOSURES REQUIRING SPECIAL AUTHORIZATION

The following disclosures require special authorization by the offices indicated:

1. Commercial Proprietary Information. Disclosure of information in this category requires the approval of the owners. Release of proprietary information is controlled by the Office of Patent Counsel (SPAWAR 00C).

2. U. S. Patent Office. Classified disclosures to the U. S. Patent Office in connection with the prosecution of application for letters of patent in behalf of the U. S. Navy require the approval of SPAWAR 00C.

3. Public News Media. Classified information shall not be disclosed through any manner of publication or presentation available or open to the public. SPAWAR 10G is responsible for coordinating with cognizant SPAWAR offices, including the Security Office, the review of material having possible public affairs or security significance.

4. Investigative Agents. Disclosures to investigative agents may not be made without prior approval of the Security Office.

5. Foreign Disclosures. The requirements for foreign sources to participate in procurement programs must be carefully reviewed to determine, at the outset, any requirements for the disclosure of U. S. classified information during the entire program cycle.

6. A detailed listing of information/documents and their classification required for bidding purposes, procurement and visits to Commands, shipyards, or areas normally restricted from access by foreign nationals must be clearly identified. The final decision (i.e., approval or denial) will be provided by the Navy Office of Technology Transfer and Security Assistance (NAVOTTSA).

7. Other Disclosures. All other classified disclosures not provided for herein shall be approved by the Security Office.

Section 3

CONTROL OF UNCLASSIFIED TECHNICAL DOCUMENTS

0311. APPLICABILITY

This section applies to unclassified technical documents. Included are the following:

1. Newly created technical documents prepared either by Government personnel or by Government contractors, including informal technical documents that contain technical data. Examples of informal technical documents are working papers, memoranda, correspondence, and preliminary reports.

2. Existing technical documents that are not already in the public domain.

3. Technical documents with superseded distribution statements.

This Section does not apply to the following types of technical documents:

a. Technical documents categorized as cryptographic and communications security, communications or electronic intelligence, and other categories designed by the Director, National Security Agency.

b. Technical documents containing Restricted Data (RD) or Formerly Restricted Data (FRD).

(These documents are controlled by the originators under a different set of rules.)

0312. DEFINITIONS

For the purpose of this Section, the following definitions apply:

1. Document. Any recorded information, regardless of its medium, physical form or characteristics.

2. Technical Data. Recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentations.

3. Critical Technology. Technology that consists of:

a. Arrays of design and manufacturing know-how (including technical data.)

b. Keystone manufacturing, inspection, and test equipment.

c. Keystone materials.

d. Goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as Military Critical Technology.)

0313. POLICY

All unclassified technical documents originated by or for this Command will be marked with one of the distribution statements listed in Exhibit 3-5 before primary distribution.

0314. RESPONSIBILITIES

1. Originating Offices. Offices originating or responsible for technical documents shall determine their distribution limitation in accordance with Exhibit 3-5. Documents to be assigned Distribution Statement A require prior approval of SPAWAR 10G.

2. Contracting Officers. Contracting Officers shall ensure that guidance is incorporated in contract documents that will enable contractors to properly mark and handle the technical documents that are generated under their contracts.

3. SPAWAR 10G. Process all technical documents recommended for Distribution Statement A as a public release in accordance with applicable public affairs regulations.

4. SPAWAR 10F. Keep abreast of all DoD policies regarding control of critical technology, maintain and keep current the Militarily Critical Technologies List (MCTL) and provide assistance and guidance to originators of technical data in determining proper distribution statement assignments.

5. Security Office

a. Provide Command oversight.

b. Serve as focal point of all requests, other than those from U. S. Government agencies and their contractors, for technical documents containing critical technology with military or space applications.

6. Procedures

a. Exhibit 3-5 describes all authorized distribution statements and provides procedures for their assignment.

b. Exhibit 3-6 provides marking instructions.

c. Exhibit 3-7 provides guidance on marking contractor controlled technical data to which the Government has limited rights.

d. All requests, other than those from U. S. Government agencies and their contractors, for technical documents containing critical technology with military or space application shall be referred to the Security Office for processing in accordance with reference (a).

e. The originator of each unclassified military specification, standard, and handbook will, as specified in paragraph 0314.1 above, assign a distribution statement to it. Such documents will, if released outside SPAWAR during the pre-solicitation stage, be reviewed for security by SPAWAR 10H prior to release. It is the responsibility of the originator to ensure this review is accomplished and made a matter of record. Exhibit 3-9 will be used to document this review.

f. SPAWAR 003-12 (Specification Advocate - SPECAD), shall ensure the appropriate distribution statement is included on unclassified specifications, standards, and handbooks processed for release. Specifications, standards, and handbooks issued by the SPECAD do not require review by SPAWAR 10G, but will be monitored by SPAWAR 10H.

g. SPAWAR 003-232 (Technical Publications Branch) shall process requests from U. S. Government agencies and their contractors for technical documents containing critical technology with military or space applications. Such request shall comply with the provisions of OPNAVINST 5510.161 concerning the qualifications of contractors.

7. Protection and Disposal. Documents marked with distribution statements B thru F.

a. Physical Protection

(1) During Duty Hours. Documents shall be controlled to ensure non-accessibility by non-Government personnel.

(2) During Non-Duty Hours. Documents shall be stored so as to preclude unauthorized access, i.e., filed in locked or unlocked files, desks, bookcases, etc.

b. Disposal. Documents shall be disposed of by defacing or destroying in such a manner that the content cannot be reconstructed.

Contract Security Classification Specification (DD Form 254) dated 1 JAN 88 for contract N00039-88-C-XXXX (Continued)

Item 15 - Remarks

Item 11g: The provisions of Sections 42, 46, and 47, ISM, apply to restricted data access required in contract performance. (This involves the design, manufacture, or utilization of atomic weapons, the production of special nuclear material, and/or use of special nuclear material in the production of energy.)

Item 11h: (Enter in Item 11o "COMSEC Account is/is not required." If required enter the following in Item 15.)

The contractor shall comply with the provisions of the NSA CSCM-1. The NSA COR has primary responsibility for the auditing of all COMSEC material governed by the CSCM-1. The cognizant security office is responsible for inspecting for compliance with the COMSEC Supplement (DoD 5220.22-S-1) to the ISM (DoD 5220.22-M.)

The contractor shall make arrangements to utilize the services of the Defense Courier System (DCS) for transportation of qualified material. The DCS station will provide guidance on what material is qualified.

Publishing or release of any COMSEC information by any means without the written approval of SPAWARSYSCOM (SPAWAR 10H) is PROHIBITED.

All subcontract DD Forms 254 involving COMSEC access must be approved by SPAWARSYSCOM (SPAWAR 10H).

Item 11i: (No longer used)

Item 11j: (If 10d is "X'd" NO, us the following remarks in Item 15.)

Access to SCI limited to that at a U. S. Government SCIF.

(If 10d is "X'd" YES, use the following remarks in Item 15.)

This contract requires access to SCI. Director of Naval Intelligence has exclusive security responsibility for such information released to the contractor or developed under this contract. DIAM 50-5 provides the necessary guidance for physical, personnel and information security measures and is a part of this security specifications for this contract. DIS is relieved of responsibility for all SCI material or information released to the contractor under this contract.

20 DEC 1988 EXHIBIT 3-1 REQUEST FOR PROPOSAL DD FORM 254

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

THIS DD 254 IS A GUIDE FOR BIDDING PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE ISSUED UPON AWARD OF CONTRACT

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: TOP SECRET

2. THIS SPECIFICATION IS FOR:	3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)	5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a)		
a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER	a.	X	a. ORIGINAL (Complete date in all cases) (RFP)	DATE 1JAN85
b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.	b.		b. REVISED (supersedes all previous specifications) REVISION NO.	DATE
X c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER N00039-85-R-0000	c. DUE DATE 31DEC85		c. FINAL	DATE

6. Is this a follow-on contract? [X] Yes [ ] No. If YES, complete the following:

a. N00039-84-C-0000 (PRECEDING CONTRACT NUMBER) b. Completed (DATE COMPLETED) c. Accountability for classified material on preceding contract

[X] Is [ ] Is not, transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
ABC Corporation 123 4th Street Alexandria, VA 22112	1B234	Director of Industrial Security 2461 Eisenhower Avenue Alexandria, VA 22331
8a. Name, Address & Zip Code of First Tier Subcontractor	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office

* When actual performance is at a location other than that specified, identify such other location

10a. General identification of the Procurement for which this specification applies ... ring Activity

c. Are there additional security requirements ... pertinent contractual documents ... identify the

d. Are any elements ... Item 1 ... Yes [ ] No. If YES, explain in

Except for the bracketed items, RFP (Requests for Proposal) DD Forms 254 shall read identical to the prospective contract DD Form 254 (Exhibit 3-2). If procurement is competitive, Items 6 and 7 would be left blank; if pre-award access to classified information is required, a list of prospective bidders must be provided to SPAWAR 10H for access/safeguarding determinations. Items 2c, 3c and 4c must be completed prior to SPAWAR 10H approval.

11.

a. Access to ... contract		
b. Receipt of ... material for referen...		
c. Receipt and ...eration of classified documents or other material.		
d. Fabrication/Modification/Storage of classified hardware.		
e. Graphic arts services only.		
f. Access to IPO information.		
g. Access to RESTRICTED DATA.		
h. Access to classified COMSEC information.		
i. Cryptographic Access Authorization required.		

ACCESS REQUIREMENTS (Continued)	YES	NO
j. Access to SENSITIVE COMPARTMENTED INFORMATION.		
k. Access to other Special Access Program information (Specify in item 15).		
l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.		
m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.		
n. Classified ADP processing will be involved.		

REMARKS:

PRE-AWARD ACCESS TO CLASSIFIED INFORMATION (IS/IS NOT) AUTHORIZED.

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official	c. Activity name, address, Zip Code, telephone number and office symbol

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions ... taken in accordance with the provisions of the Industrial Security Manual.

DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE. S/N 0102-LF-000-2540

THIS DD 254 IS A GUIDE FOR BIDDING PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE ISSUED UPON AWARD OF CONTRA

EXHIBIT 3-2

20 DEC 1988

ORIGINAL CONTRACT DD FORM 254

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)	5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a)			
X	a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER N00039-88-C-0000	a. 30SEP90	X	a. ORIGINAL (Complete date in all cases)		DATE 1JAN88
	b. SUBCONTRACT (Use item 15 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.	b.		b. REVISED (supersedes all previous specifications)	REVISION NO.	DATE
	c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER N00039-88-R-0000	c. DUE DATE		c. FINAL		DATE

6. Is this a follow-on contract? [X] Yes [ ] No. If YES, complete the following:

a. N00039-84-C-0000 (PRECEDING CONTRACT NUMBER) b. COMPLETED (DATE COMPLETED) c. Accountability for classified material on preceding contract

[ ] is [ ] is not, transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
ABC CORPORATION 123 4th Street Alexandria, VA 22221	1A234	Director of Industrial Security 2461 Eisenhower Avenue Alexandria, VA 22331
8a. Name, Address & Zip Code of First Tier Subcontractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office

* When actual performance is at a location other than that specified, identify such other location in Item 15.

10a. General identification of the Procurement for which this specification applies	b. DoDAAD Number of Procuring Activity identified in Item 16d.
AN/WLR-100 Production and Engineering Services	N00039

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? [X] Yes [ ] No. If YES, identify the pertinent contractual documents in Item 15. (this item used only with Items 11j & 11k below)

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? [X] Yes [ ] No. If YES, explain in Item 15 and identify specific areas or elements (this item used only with Items 11j & 11k below)

11. ACCESS REQUIREMENTS	YES	NO	ACCESS REQUIREMENTS (Continued)	YES	NO
a. Access to Classified Information Only at other contractor/Government activities.	X		j. Access to SENSITIVE COMPARTMENTED INFORMATION.	X	
b. Receipt of classified documents or other material for reference only (no generation)	X		k. Access to other Special Access Program information (Specify in Item 15).	X	
c. Receipt and generation of classified documents or other material.	X		l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.	X	
d. Fabrication/Modification/Storage of classified hardware.	X		m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.	X	
e. Graphic arts services only.		X	n. Classified ADP processing will be involved.	X	
f. Access to IPO information. (NATO)	X		o. REMARKS: Intelligence documents - See Item 15		
g. Access to RESTRICTED DATA.	X				
h. Access to classified COMSEC information.	X				
i. Cryptographic Access Authorization required.		X			

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official	c. Activity name, address, Zip Code, telephone number and office symbol
	Space & Naval Warfare Systems Command SPAWAR 10H Washington, D.C. 20363-5100 (202)692-8651

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE S/N 0102-LF-000-2540

20 DEC 1988

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5a and Appendix IX).

b. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify):

Commander, Space & Naval Warfare Systems Command (SPAWAR 10G) Washington D.C. 20363-5100

Public Release of SCI is not authorized.

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review in accordance with paragraph 5a of the Industrial Security Manual.

* In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.

14. Security Classification Specifications for this solicitation/contract are identified below ("X" applicable box(es) and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (if applicable).

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☐ a. A completed narrative is (1) ☐ attached, or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached, or (2) ☐ transmitted under separate cover. (List guides under Item 15 or in an attachment by title, reference number and date).

☐ c. Service-type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate.).

☐ d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____.

☐ e. Biennial review of this DD Form 254 is required. If "X'd", provide date such review is due: _____.

15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions).

(The following remarks correspond to various items and must be typed in Item 15 and continued on a separate page when additional space is required.)

Item 7a: (When contract performance is located at a contractor's address other than that listed in Item 7a, the address and FSC number must be indicated here.)

Item 11a: This is a service contract. Review or final DD Form 254 will not be issued. (Para 60h, ISM.)

Item 11b: This is a service contract. DD Form 254 review will not be conducted. A final DD Form 254 will be issued stating disposition of classified received.

Item 11c: The attached "TEMPEST SECURITY REQUIREMENTS" is imposed if any electrical processing of SECRET/TOP SECRET information is involved in contract performance

Item 11d: (Indicate nomenclature/classification/cubic feet or space required for classified GFE storage.)

Item 11e: (NOT USED)

Item 11f: This contract requires access to classified NATO information. The requirements of Section XI, ISM, shall be complied with in the handling of such information.

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16c below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.

REQUIRED DISTRIBUTION:

☒ Prime Contractor (Item 7a)
☒ Cognizant Security Office (Item 7c)
☒ Administrative Contracting Office (Item 16a)
☐ Quality Assurance Representative
☐ Subcontractor (Item 8a)
☐ Cognizant Security Office (Item 8c)
☒ Program/Project Manager (Item 12b)
☐ U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

☒ SPAWAR 10H
☒ SPAWAR 00H; NIC 44 (when SCI involved)
☒ NSA (Y-131) (when COMSEC account required)

b. Typed name and title of approving official
C.W. PHILBRICK
Contracting Officer for Security Matters

c. Signature

d. Approving official's activity address and Zip Code
Space & Naval Warfare Systems Command
(SPAWAR 10H)
Washington, D.C. 20363-5100 (202) 692-8667

e. Name, address and Zip Code of Administrative Contracting Office
Same as Item 6, SF 26

U.S. Government Printing Office 1984—765-612/15864 5-1

S/N0102-LF-009-2540

This contract requires the use of the Defense Courier System (DCS).

Item 11k: This requires CNWDI (Critical Nuclear Weapons Design Information) access. (See Section XIV, ISM.)

-or-

(Enter any other Special Access Programs and CNO (OP-090) approval document.)

Item 11l: Section XII, ISM, shall apply to all contractor personnel aboard U. S. Flag or Foreign Flag vessels at sea, or assigned ashore duty overseas.

Item 11m: DTIC Services authorized. Submit DD Forms 1540 and 1541 in accordance with Appendix I, ISM.

Item 11n: The provisions of Section XIII, ISM, pertain to the classified ADP processing actions required in contract performance.

Item 11o: The following conditions of release apply to Intelligence documents:

1. The material does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all foreign intelligence released and any material using data from such intelligence shall be returned to the Contracting Officer or authorized representative for final disposition. Only with prior authorization from the Commander, Naval Intelligence Command (NIC-52) may the contractor retain such material.

2. Contractor personnel will not release the foreign intelligence material to any activity or person of the contractor's organization not directly engaged in providing services under the contract or to another contractor (including subcontractors), government agency, private individual, or organization without prior approval of the Commander, Naval Intelligence Command (NIC-52).

3. Foreign intelligence material will not be released to foreign nationals or immigrant aliens who may be employed by the contractor, regardless of the level of their security clearance except with the specific permission of the Commander, Naval Intelligence Command (NIC-52).

4. Foreign intelligence material may not be reproduced without prior approval from the Commander, Naval Intelligence Command (NIC-52). All foreign intelligence material must bear a prohibition against reproduction while in the custody of the contractor.

5. The contractor shall maintain such records as will permit him to furnish, on demand, the names of individuals who have access to foreign intelligence material in his custody.

Item 15 - Remarks

Item 14a(1): This is a study contract. Material generated under this contract shall perpetuate the classification/downgrading/declassification of the source material. The highest classification for this contract is TOP SECRET.

-or-

This is a research contract. The highest level of classification for this contract as a whole is TOP SECRET. A revised DD Form 254 will be issued as soon as possible to provide detailed security classification guidance.

-or-

Material generated under this contract shall perpetuate the classification/downgrading/declassification of the source material, the highest level of classification for this contract is TOP SECRET.

Item 14b(1): OPNAVINST S5513.8A, enclosure (33), ID: 08A-33, subj: AN/WLR-100 (3 unclassified pages)

-or-

Item 14b(2): OPNAVINST S5513.8A, enclosure (33), ID: 08A-33, subj: AN/WLR-100 (3 Secret pages)

-or-

(Any other officially approved classification guide.)

Contract Security Classification Specification (DD Form 254) dated 1 JAN 88
for contract N00039-88-C-XXXX (Continued)

The following general remarks shall appear on all DD Forms 254:

Information on this contract is not releasable to personnel possessing reciprocal clearances without the written approval of SPAWARSYSCOM (SPAWAR 10H) (see para. 31, ISM.)

Visit requests to activities other than SPAWARSYSCOM shall have "NEED-TO-KNOW" certified by SPAWARSYSCOM (insert project code)....All requests shall contain the information required by para. 37d, ISM, and shall not exceed the date indicated in Item 4, or a 12-month period, whichever is earlier.

C. W. PHILBRICK
Contracting Officer for Security Matters
Space and Naval Warfare Systems Command
(SPAWAR 10H)
Washington, D.C. 20363-5000
(202) 692-8667

2 0 DEC 1988

EXHIBIT 3-3
REVISED DD FORM 254

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: TOP SECRET

2. THIS SPECIFICATION IS FOR:	3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)	5. THIS SPECIFICATION IS: (See "NOTE" below. If Item b or c is "X'd", also enter date for Item a)		
a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER	a.	a. ORIGINAL (Complete date in all cases)		DATE 10CT84
b. SUBCONTRACT (Use Item 13 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.	b.	X b. REVISED (supersedes all previous specifications)	REVISION NO. 1	DATE 1JAN85
c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER	c. DUE DATE	FINAL		DATE

6. Is this a follow-on contract? ☐ Yes ☐ No. If YES, complete the following:

a. _____ PRECEDING CONTRACT NUMBER b. _____ DATE COMPLETED c. Accountability for classified material on preceding contract

☐ is ☐ is not, transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
8a. Name, Address & Zip Code of First Tier Subcontractor *	b. FSC Number	c. Name, Address & Zip Code of Cogni- [illegible] e
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *	b. FSC Number	c. Name [illegible] ugnizant Security Office

* When actual performance is at a location other than that [illegible] location in Item 15.

10a. General identification of the Procurement for wh[illegible] b. DoDAAD Number of Procuring Activity identified in Item 16d.

c. Are there additional secur[illegible] in accordance with paragraph 1-114 or 1-115, ISR? ☐ Yes ☐ No. If YES, identify the pertinent contractual [illegible]

d. Are any elem[illegible] the inspection responsibility of the cognizant security office? ☐ Yes ☐ No. If YES, explain in Item 13 [illegible] or elements.

A revised DD Form 254 is required when security requirements change; when the date in Item 4 expires, etc. The revised DD Form 254 will reflect the information in Exhibit 3-2, as required, except for Item 5 (bracketed) above.

11. [illegible] REQUIREMENTS	YES	NO	ACCESS REQUIREMENTS (Continued)	YES	NO
a. Access to [illegible]ified Information Only at other contractor/Government activities.			j. Access to SENSITIVE COMPARTMENTED INFORMATION.		
b. Receipt of classified documents or other material for reference only (no generation).			k. Access to other Special Access Program information (Specify in Item 13).		
c. Receipt and generation of classified documents or other material.			l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.		
d. Fabrication/Modification/Storage of classified hardware.			m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.		
e. Graphic arts services only.			n. Classified ADP processing will be involved.		
f. Access to IPO information.			o. REMARKS:		
g. Access to RESTRICTED DATA.					
h. Access to classified COMSEC information.					
i. Cryptographic Access Authorization required.					

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official	c. Activity name, address, Zip Code, telephone number and office symbol

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

S/N 0102-LF-000-2540

DD FORM 1 JAN 78 254 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

EXHIBIT 3-4
FINAL DD FORM 254

2 0 DEC 1988

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: TOP SECRET

2. THIS SPECIFICATION IS FOR:		b. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	c. DATE TO BE COMPLETED (Estimated)	3. THIS SPECIFICATION IS: (See "NOTE" below. If Item b or c is "X", also enter date for Item a)		
X	a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER N00039-85-C-XXXX	a. COMPLETED		a. ORIGINAL (Complete date in all cases)	DATE 10NOV83
	b. SUBCONTRACT (Use Item 13 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.	b.		b. REVISED (supersedes all previous specifications) REVISION NO. 1	DATE 31OCT84
	c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER	c. DUE DATE	X	c. FINAL	DATE 20JAN85

4. Is this a follow-on contract? ☒ Yes ☐ No. If YES, complete the following:
a. N00039-82-C-XXXX (PRECEDING CONTRACT NUMBER) b. COMPLETED (DATE COMPLETED) c. Accountability for classified material on preceding contract
☒ is ☐ is not, transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
ABC Corporation 123 4th Street Arlington, VA XXXXX	1A234	Director of Industrial Security 2461 Eisenhower Avenue Alexandria, VA 22331
8a. Name, Address & Zip Code of First Tier Subcontractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office

* When actual performance is at a location other than that specified, identify such other location in Item 13.

10a. General identification of the Procurement for which this specification applies: AN/WLR-500 Engineering Developmemt Model

b. DoDAAD Number of Procuring Activity identified in Item 16d: N00039

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISM? ☐ Yes ☒ No. If YES, identify the pertinent contractual documents in Item 13.

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? ☐ Yes ☒ No. If YES, explain in Item 13 and identify specific areas or elements.

11. ACCESS REQUIREMENTS	YES	NO	ACCESS REQUIREMENTS (Continued)	YES	NO
a. Access to Classified Information Only at other contractor/Government activities.			j. Access to SENSITIVE COMPARTMENTED INFORMATION.		
b. Receipt of classified documents or other material for reference only (no generation).			k. Access to other Special Access Program information (Specify in Item 13).		
c. Receipt and generation of classified documents or other material.			l. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.		
d. Fabrication/Modification/Storage of classified hardware.			m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.		
e. Graphic arts services only.			n. Classified ADP processing will be involved.		
f. Access to IPO information.			o. REMARKS:		
g. Access to RESTRICTED DATA.					
h. Access to classified COMSEC information.					
i. Cryptographic Access Authorization required.					

12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e)) EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/project manager or other designated official
John Q. Doe
Project Manager

c. Activity name, address, Zip Code, telephone number and office symbol
Space and Naval Warfare Systems Command
(PMW107-8)
Washington, DC 20363-5100
(202) 692-XXXX

NOTE: Original Specification (Item 3a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 3b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

DD FORM 1 JAN 79 254 — EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

S/N 0102-LF-000-2540

20 DEC 1988

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5o and Appendix IX).

b. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify):

Commander, Space & Naval Warfare Systems Command (SPAWAR 10G) Washington, D.C. 20363-5100

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review in accordance with paragraph 5o of the Industrial Security Manual.

* In the case of non-DoD User Agencies, see footnote, paragraph 5o, Industrial Security Manual.

14. Security Classification Specifications for this solicitation/contract are identified below ("X" applicable box(es) and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:
(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (If applicable).

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☐ a. A completed narrative is (1) ☐ attached, or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached, or (2) ☐ transmitted under separate cover. (List guides under Item 13 or in an attachment by title, reference number and date).

☐ c. Service-type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate.).

☐ d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____.

☐ e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____.

15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions).

(Disposition of all classified material received or generated by the contractor must be indicated in this section. Select or modify the examples below to fit the situation.)

In response to ABC Corporation letter XXX:jf:ei dated 30NOV84, all classified material received or generated under this contract may be retained for a period of (up to 5 years)

All classified material received or generated under this contract may be retained for a period of (up to 5 years) provided no cost to the U.S. Government is incurred.

All classified material received or generated under this contract shall be returned to the Contracting Officer's Technical Representative.

All classified material received or generated under this contract shall be destroyed in accordance with the provisions set forth in the Industrial Security Manual.

All classified material received or generated under this contract shall be transferred to the accountability of contract N00039-87-C-XXXX.

Information on this contract is not releasable to personnel possessing reciprocal clearances without the written approval of COMSPAWARSYSCOM (SPAWAR 10H) (see para 31, ISM).

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.

REQUIRED DISTRIBUTION:

☒ Prime Contractor (Item 7a)
☒ Cognizant Security Office (Item 7c)
☒ Administrative Contracting Office (Item 16e)
☐ Quality Assurance Representative
☐ Subcontractor (Item 8a)
☐ Cognizant Security Office (Item 8c)
☒ Program/Project Manager (Item 12b)
☐ U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

☒ SPAWAR 10H (plus distribution listed on active DD Form 254)
☐
☐

b. Typed name and title of approving official
C.W. PHILBRICK
Contracting Officer for Security Matters

c. Signature

d. Approving official's activity address and Zip Code
Space & Naval Warfare Systems Command
(SPAWAR 10H)
Washington, D.C. 20363-5100 (202) 692-8667

e. Name, address and Zip Code of Administrative Contracting Office

Same as Item 6, SF 26

U.S. Government Printing Office: 1984—706-012/15884 2-1 S/N0102-LF-000-2540

EXHIBIT 12B

PROCEDURES FOR ASSIGNING DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS

PROCEDURES

1. Newly generated unclassified technical documents will be assigned Distribution Statement A, B, C, D, E, F, or X. Existing unclassified technical documents will be assigned Distribution Statement A, B, C, D, E, F or X if they have not already been made generally available to the public and if they are likely to be disseminated outside the Department of Defense. Technical documents in preliminary or working draft form will not be disseminated without a proper security classification review and assignment of a distribution statement.

2. Classified technical documents will be assigned Distribution Statement B, C, D, E or F. The distribution statement assigned to a classified document will be retained on the document after declassification or until the originating command specifically changes or removes it. If a technical document without a distribution statement is declassified, it will be handled the same as Distribution Statement F documents until changed by the originating command.

3. If a newly generated technical document contains export-controlled technical data, it will be marked with the statement in paragraph 1 under "ADDITIONAL NOTICES", in addition to Distribution Statement B, C, D, E, F or X.

4. Scientific and technical documents which include a contractor-imposed "limited rights" statement will be appropriately marked and controlled. (See "CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS" below.)

5. The distribution statement will be displayed conspicuously so it will be recognized readily by recipients. For standard written or printed material, the distribution statement will appear on the front cover, title page, and DD Form 1473, "Report Documentation Page". When possible, parts that contain information creating the requirement for the distribution statement will be prepared as an appendix to permit broader distribution of the basic document. When practicable, the abstract of the document, the DD Form 1473 and bibliographic citations will be written in such a way that the information will not be subject to Distribution Statement B, C, D, E, F or X. If the technical information is not in standard written or printed form and does not have a cover or title page, the distribution statement will be conspicuously stamped, printed, written or affixed by other means.

6. Distribution statements remain in effect until changed or removed by the originating command. Each command will establish and maintain a procedure for review of technical documents for which it is responsible, with the objective

of increasing their availability as soon as conditions permit. Public release determinations will be processed in accordance with references (cc) and (dd). When public release clearance is obtained, Distribution Statement A will be assigned and document handling facilities, including Defense Technical Information Center (DTIC), will be notified.

7. Technical documents with superseded distribution limitation markings will be reviewed and assigned the appropriate distribution statement when a request for the document is received. Superseded distribution limitation markings will be converted as follows:

a. Documents with distribution marking A or B need not be re-evaluated or remarked.

b. Documents with distribution marking #2 will be assigned Distribution Statement C.

c. Documents with distribution marking #3 (U.S. Government Only) will be assigned Distribution Statement B.

d. Documents with distribution marking #4 (DOD Only) will be assigned Distribution Statement E.

e. Documents with distribution marking #5 (Controlled) will be assigned Distribution Statement F.

8. Originating commands will promptly notify Defense Technical Information Center and other information repositories holding their technical documents when:

a. Address of designated originating commands is changed.

b. The originating command is redesignated.

c. Classification markings, distribution statements or export control statements are changed.

DISTRIBUTION STATEMENTS

The following distribution statements are authorized for use on technical documents:

1. **DISTRIBUTION STATEMENT A:** Approved for public release; distribution is unlimited.

a. This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority in accordance with references (cc) and (dd).

b. Technical documents resulting from contracted fundamental research efforts will normally be assigned Distribution Statement A, except for those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded in the contract or grant.

c. Technical documents with this statement may be made available or sold to the public including foreign nationals, companies, and governments, and may be exported.

d. This statement may never be used on technical documents that formerly were classified without a positive determination of such releasability by the command exercising cognizance over the information prior to release.

e. THIS STATEMENT WILL NOT BE USED ON CLASSIFIED TECHNICAL DOCUMENTS OR DOCUMENTS CONTAINING EXPORT-CONTROLLED TECHNICAL DATA AS PROVIDED IN OPNAVINST 5510.161 REFERENCE (jj).

2. **DISTRIBUTION STATEMENT B:** Distribution authorized to U.S. Government agencies only; (fill in reason) (date). Other requests for this document must be referred to (insert originating command).

a. This statement may be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement B include:

Foreign Government - To protect and limit information distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type is normally classified at the CONFIDENTIAL level or higher.

Proprietary Information - To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it may not be routinely transmitted outside the U.S. Government.

Critical Technology - To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of OPNAVINST 5510.161, reference (jj).

Test & Evaluation - To protect results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

Contractor Performance Evaluation - To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Premature Dissemination - To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.

Administrative/Operational Use - To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation - Releasable only in accordance with the provisions of SECNAVINST 5237.2 (NOTAL), reference (kk).

Specific Authority - To protect information not specifically included in the above reasons, and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DOD or DON regulations or policy guidance. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

3. **DISTRIBUTION STATEMENT C:** Distribution authorized to U.S. Government agencies and their contractors; (fill in reason) (date). Other requests for this document will be referred to (insert originating command).

a. May be used on unclassified technical documents, or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement C include:

(1) Foreign Government Information - Same as Distribution Statement B.

(2) Critical Technology - Same as Distribution Statement B.

(3) Software Documentation - Same as Distribution Statement B.

(4) Administrative or Operational Use - Same as Distribution Statement B.

(5) Specific Authority - Same as Distribution Statement B.

4. **DISTRIBUTION STATEMENT D:** Distribution authorized to DOD and DOD contractors only; (fill in reason) (date). Other U.S. requests shall be referred to (insert originating command).

a. May be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement D include:

(1) Foreign Government Information - Same as Distribution Statement B.

(2) Administrative or Operational Use - Same as Distribution Statement B.

(3) Software Documentation - Same as Distribution Statement B.

(4) Critical Technology - Same as Distribution Statement B.

(5) Specific Authority - Same as Distribution Statement B.

5. **DISTRIBUTION STATEMENT E:** Distribution authorized to DOD components only; (fill in reason) (date). Other requests must be referred to (insert originating command).

a. May be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement E include:

(1) Direct Military Support - Document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States. Designation of such data is made by competent authority in accordance with OPNAVINST 5510.161, reference (jj).

(2) Foreign Government Information - Same as Distribution Statement B.

(3) Proprietary Information - Same as Distribution Statement B.

(4) Premature Dissemination - Same as Distribution Statement B.

(5) Test and Evaluation - Same as Distribution Statement B.

(6) Software Documentation - Same as Distribution Statement B.

(7) Contractor Performance Evaluation - Same as Distribution Statement B.

(8) Critical Technology - Same as Distribution Statement B.

(9) Administrative/Operational Use - Same as Distribution Statement B.

(10) Specific Authority - Same as Distribution Statement B.

6. **DISTRIBUTION STATEMENT F:** Further dissemination only as directed by (insert originating command) (date) or higher DOD authority.

a. Normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists.

b. Distribution Statement F is used when the originator determines that the information is subject to the special dissemination limitation specified by paragraph 9-32.2a.

c. When a classified document assigned Distribution Statement F is declassified, the statement will be retained until the originating command assigns the proper distribution statement.

7. **DISTRIBUTION STATEMENT X:** Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with OPNAVINST 5510.161, reference (jj). Other requests must be referred to (originating command).

a. This statement will be used on unclassified documents when Distribution Statements B, C, D, E or F are not applicable but the document contains technical data as explained in OPNAVINST 5510.161, reference (jj).

b. This statement will not be used on classified technical documents. It may be assigned to technical documents that formerly were classified.

ADDITIONAL NOTICES

In addition to the distribution statement, the following notices will be used when appropriate:

1. All technical documents determined to contain export-controlled technical data will be marked "WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec. 2751 **et seq.**) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App 2401, **et seq.** Violations of these export laws are subject to

severe criminal penalties. Disseminate in accordance with provisions of OPNAVINST 5510.161, reference (jj)." When it is technically infeasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data" required by OPNAVINST 5510.161, reference (jj).

2. **Handling and Destroying Unclassified/Limited Distribution Documents.** Unclassified/Limited Distribution documents shall be handled using the same standard as "For Official Use Only (FOUO)" material, and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicate that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balanced against the degree of sensitivity.

CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS

1. Contractors may have proprietary technical data to which the Government is given limited rights. The contractor will place a limited rights statement on each document containing contractor-controlled technical data furnished to the Government. Documents with limited rights information will be assigned Distribution Statements B, E, or F.

2. Limited rights is defined as the right to use, duplicate, or disclose technical data in whole or in part, by or for the U.S. Government with the expressed limitation that, such technical data, without the written permission of the party furnishing the technical data, may not be:

a. Released or disclosed in whole or in part outside the Government.

b. Used in whole or in part by the Government for manufacture, or in the case of computer software documentation, for reproduction of the computer software.

c. Used by a party other than the Government, except for:

(1) Emergency repair or overhaul work only by or for the Government, when the item or process concerned is not otherwise reasonably available to enable timely performance of the work, provided that the release or disclosure outside the Government will be made subject to a prohibition against further use, release or disclosure, or

(2) Release to a foreign government, as the interest of the United States may require, only for information or evaluation within the foreign government or for emergency repair or overhaul work by or for the foreign government under the conditions of subparagraph (1).

3. The limited rights statement remains in effect until changed or cancelled under contract terms or with the permission of the contractor and the controlling office notifies recipients of the document that the statement has been changed or cancelled. Upon cancellation of the limited rights statement, the distribution, disclosure, or release of the technical document will then be controlled by its security classification or, if it is unclassified, by assignment of the appropriate Distribution Statement.

EXHIBIT 3-8

MEMORANDUM

From: _____
(Sponsoring Office)

To: SPAWAR 18-51

Subj: CERTIFICATION OF NEED AND SECURITY CLEARANCE FOR REMOVAL OF CLASSIFIED MATERIAL FROM SPAWAR BY REPRESENTATIVES OF OTHER ACTIVITIES

1. It is requested that _____ be authorized
(Name of Courier)
to receipt for and hand-carry the following classified material from this Command:

2. The need for this request has been carefully considered and evaluated and the following certifications made:

a. This release is in direct support and benefit to SPAWAR and not for the sole convenience of the recipient.

b. Use of normal mail transmission channels would not permit delivery in time to meet SPAWAR objectives.

c. The recipient has a security clearance and storage capabilities to the same degree or higher than the classified material involved. The security clearance of the courier is likewise certified.

d. The material identified above is required by the recipient for:

____ Project/Program (indicate by name) _____

____ Contract Performance (indicate Contract No.)_____
_____

____ Pre-contract negotations (indicate IFB, RFQ, RFP, etc.)_____

NOTE: The sponsoring office is responsible for ensuring clearances have been verified and are on file. The sponsoring office shall contact the Security Office if clearance data has not been previously furnished.

_____
Signature - (individual having
By direction authority)

Copy to:
SPAWAR 10H1

20 DEC 1983

ROUTE SLIP AND OFFICE MEMO
SPAWAR 5216/1 (Rev. 9-85)

DO NOT [illegible] CORRESPONDENCE.
WRITE ON PRINT [illegible]

CONTROL NO.	REPLY DUE BY			
ORIGINATOR *(Code, and Extension when applicable)*	SERIAL	DATE	SUBJECT CLASS	CROSS REF.

ROUTE TO CODE	SYMBOL	RELEASED INITIAL	DATE MON.	DAY	YEAR	SUBJECT REVIEW OF MILSPEC/STD/HANDBOOK EXHIBIT 3-9 / ENCLOSURE
						SIGNATURE, EXT. CODE AND DATE ARE TO FOLLOW COMMENTS SYMBOLS: A- Action C - Comment I - Information P - Prepare Reply R - Retain Copy
10H						The attached document is forwarded for review in accordance with
						paragraph 0314.6E of SPAWARINST 5510.3G. The purpose of this
						review is to ensure that the document may be released outside
						SPAWAR during the pre-solicitation stage.
						Answer the questions below prior to forwarding the request to
						SPAWAR 10H for review:
						A. Would release of this information reveal any critical technolo
						YES NO
						B. Does it contain information of potential intelligence value?
						YES NO
						C. What significant benefits will be derived by the Navy by its
						release?
						D. Was the material developed under SPAWAR/NAVELEX contract
						and if so, what number?
						E. Should the sponsor review this document? If so, please
						indicate name and code of sponsor.
						F. Comments:
						Signature/Code of Originator
						10H Action: Approve/Disapprove

FILE	UNLESS THIS MATERIAL IS TO BE FURTHER ROUTED – RETURN TO FILE BY DATING AND INITIALING.	INITIAL	DATE

CHAPTER IV

PERSONNEL SECURITY AND SPECIAL ACCESS AUTHORIZATION

Section 1

PERSONNEL SECURITY CLEARANCES

0401. GENERAL

1. A personnel security clearance is an administrative determination that an individual is eligible from a security standpoint for access to classified information.

2. Executive Order 10450, as amended, states that the interests of the national security require that all persons privileged to be employed in the Navy shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. That order requires an effective program to ensure that the employment or retention in employment of any civilian employee is clearly consistent with the interests of the national security. Although Executive Order 10450 applies to civilian employees, the same criteria apply to military personnel and are promulgated by the Naval Military Personnel Command (NMPC).

0402. RESPONSIBILITIES

1. Military Personnel

The granting of personnel security clearances is a Command function. The Director, Security Office is authorized, in the name of the Commander, to grant appropriate security clearances for Headquarters military personnel.

2. Civilian Personnel

Final clearances for civilian personnel are granted by the Central Adjudication Facility (CAF), a component of the Navy Investigative Service Command (NISCOM). The Director, Security Office is enpowered to grant interim clearances as part of the clearance processing procedure.

0403. POSITION SENSITIVITY

1. Security clearance and investigative requirements for civlian employees are predetermined based on degree of access required and the category of sensitivity assigned to the position to be occupied. The categories of sensitivity as defined in Civilian Manpower Management.

2. Critical Sensitive. A critical-sensitive position is any sensitive position other than those in the non-critical-sensitive category, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security. Such positions will include: any position the duties of which include access to Top Secret information; involved in development of approval of plans, policies, or programs that affect the overall operations of the Department of the Navy; involved in development or approval of war plans, plans or particulars of future major or special operational of war, or critical and extremely important items of war; involved in investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations; assigned to fiduciary, public contact, or other duties demanding the highest degree of public trust; assigned to duties requiring access to Sensitive Compartmented Information (SCI); any other position so designated by the Director, Security Office. A person occupying a critical-sensitive position will require a Background Investigation-Period Re-Investigation (BI-PR) for BIs over five (5) years old and at five (5) year intervals for continued access to Top Secret.

3. Noncritical-Sensitive. A noncritical-sensitive position is any sensitive position other than those in the critical-sensitive category, the occupant of which could bring about by virtue of the nature of the position, a material adverse effect on the national security. Such positions will include: all positions, the duties or responsibilities of which require 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 category II automated data program positions; any other position so designated by the Secretary of the Navy or his designees.

4. The level of clearance is determined by the actual degree of classified access required in performance of official duties.

5. Non-Sensitive. All other positions in SPAWAR (i.e., those requiring no clearance) will be designated as non-sensitive.

0404. PRE-HIRE SECURITY PROCESSING (CIVILIAN)

1. All requests for personnel action require the initiation of a Standard Form SF-52, "Request for Personnel Action." All offices initiating a SF-52 for

a transfer or recruitment action, will enter in Item 3 the degree of access required and the sensitivity category of the position. CCPO will not effect appointment of individuals (applicants, transfers, etc.) to SPAWAR positions until receipt of notification from the Security Office that the necessary security requirements have been satisfied. This notification will be made by initialling the SF-52. If derogatory information is surfaced, the Security Office will notify the hiring code.

2. In cases of emergency, sensitive positions may be filled pending the completion of the required investigation if such action is necessary in the interest of national security. If an exception is required, the employing office must request the exception by memorandum to the Director, Security Office stating that it is in the interest of national security that an exception be made and giving the basis therefore. A person hired under such conditions may not be eligible for a clearance until investigative requirements are met.

0405. PROCEDURES

1. Based on position sensitivity (see para. 0403) the hiring code may request a clearance. The request will be prepared in accordance with Exhibit 4-1 and be submitted as follows:

a. Top Secret. Authority to request clearance at this level is limited to Deputy Commander, Assistant Commanders, Program Directors and Heads of Staff Offices. This authority cannot be redelegated.

All requests for Top Secret (TS) clearances received by SPAWAR 10H will be logged in and handcarried to SPAWAR 00H. SPAWAR 00H is to indicate whether or not Sensitive Compartmented Information (SCI) is required and handcarry back to SPAWAR 10H.

If 00H indicates SCI is required 10H will:

(1) Prepare an OPNAV Form 5510/413T to include the granting of an interim TS clearance.

(2) Forward the original Form 5510/413T to 00H for inclusion in the SCI access request package.

(3) Maintain a file copy of the 5510/413T as evidence of interim TS clearance and notify the requesting code of the clearance issue.

b. Secret/Confidential. Authority to request clearances at these levels is limited to Division Directors or equivalent. This authority cannot be redelegated.

2. Reserve Military Personnel. Reserve military personnel are cleared by their respective reserve units, and the degree of clearance is indicated on active duty for training orders.

0406. UPGRADING CLEARANCES

When there is need to upgrade a clearance, a request should be submitted to the Security Office furnishing name of employee and justification for the requested actions as outlined in Exhibit 4-1.

0407. DOWNGRADING/WITHDRAWAL OF CLEARANCE

Supervisors are required to identify any employee in their organization whose duties do not require access to classified information. Submit a memorandum to the Security Office indicating the name of the individual and the required clearance level of withdrawal. Action will be taken by this office to administratively downgrade/withdraw the individual's clearance. This action is non-prejudical and in no way affects the individual's future eligibility for access. If access is required at a later date, submit your request in the format of Exhibit 4-1 via the Program Director, Deputy Commander, Assistant Commander or Staff Office Head, as appropriate.

0408. SECURITY INDOCTRINATION

Every new employee is given a basic security indoctrination by the Security Office. In addition, every supervisor, assisted by the Directorate or Division Security Coordinator, provides such security instruction as is necessary to ensure compliance with Command security regulations. These instructions are to be on a continuous day-to-day basis.

0409. SECURITY AGREEMENT

1. Upon completion of the basic security indoctrination and prior to clearance being granted, each new employee executes a statement acknowledging that security directives have been made known to him and that he/she agrees to abide by the requirements specified. This statement is retained by the Security Office for the duration of employment with SPAWAR.

2. Every individual in SPAWAR Headquarters is required to have on file in the Security Office, a current DD 398, Personnel Security Questionnaire. The DD 398 is required to be updated every five years, is used in making access

determinations, and is retained in the Security Office for the duration of employment with SPAWAR. No clearance will be issued until this form has been received by the Security Office.

0410. TERMINATION OF CLEARANCE

Security clearances are terminated when: A person discontinues employment; is temporarily separated for a period of 60 days or more (including sabbaticals and leave without pay); when the requirements of the position are changed so that access to classified matter is no longer required or clearance in a lesser degree would suffice; as a result of the findings of a security board. Upon termination of clearance, the employee signs a statement indicating that he will not disclose any classified information made available to him while in the employ of SPAWAR unless specifically authorized by the Department of the Navy. Civilian personnel termination statements will be retained by the Security Office for a period of two years. It is the responsibility of the supervisory personnel concerned to keep the Security Office fully informed when an employee transfers to another position, when there is a change in clearance requirements, or any factors/conditions which may be cause to withhold access to classified matter. The following paragraph outlines examples of factors regarding an employee, which may preclude a finding that continuation of clearance is clearly consistent with the interests of the national security.

0411. FACTORS AFFECTING PERSONNEL SECURITY CLEARANCES

Supervisory personnel will thoroughly familiarize themselves and their subordinates with the factors affecting personnel security clearances; ensure that all personnel understand the necessity of reporting to the Security Office any factors/indicators observed which may preclude continuing an employee's access to classified information.

1. Financial Irresponsibility. Failure to meet just and avoidable financial obligations voluntarily incurred.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) History of bad debts and unmanageable indebtedness.

(2) Recent bankruptcy with continuing financial problems.

(3) Indebtedness aggravated or caused by gambling, alcohol, drug abuse, or mental or emotional defects.

(4) A history of pattern of writing checks not covered by sufficient funds.

(5) Unfavorable judgements, liens, or repossessions.

(6) Deceit or deception, embezzlement, or change of address without advising creditors.

(7) Applicant's indifference to financial obligations or a stated intention not to meet these obligations in the future.

(8) Financial mismanagement or irresponsibile expenditures that exceed income or other assets.

2. Criminal Conduct. Any criminal violation of a federal, state, or local law.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Criminal conduct involving:

(a) Force, coercion, or intimidation.

(b) Firearms or explosives.

(c) Dishonesty or false statements.

(d) Obstruction or corruption of Government functions.

(e) Deprivation of civil rights.

(f) Violence against persons or property.

(2) Criminal conduct punishable by confinement for one year or more.

(3) An established pattern of criminal conduct.

(4) Failure to complete a rehabilitation program resulting from disposition of a criminal proceeding.

(5) Criminal conduct that is so recent in time as to preclude a determination that recurrence is unlikely.

(6) Close and continuing association with persons known to be involved in criminal activities.

(7) Criminal conduct indicative of a serious mental abberation, lack of remorse, or insufficient probability of rehabilitative success.

(8) Disposition

(a) Conviction.

(b) Disposition on a legal issue not going to the merits of the crime.

(c) Arrest or indictment pending trial.

(9) Arrest Record. In evaluating an arrest record, information that indicates that the individual was acquitted, that the charges were dropped or the subject of a stet or nolle prosequi, that the record was expunged, or that the case was dismissed due to error not going to the merits does not necessarily negate the security significance of the indictment. Personnel security determinations are to be made on the basis of all available information concerning a person's conduct and actions rather than the legal outcome of a criminal proceeding.

3. Sexual Misconduct. Sexual behavior that makes applicable the guidance for criminal misconduct or mental or emotional illness, or which indicates that the applicant may be subjected to coercion, pressure, or influence to act contrary to the interests of the United States or which suggests recklessness, irresponsibility, or poor judgement.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) The misconduct has been recent or frequent.

(2) The applicant indicates explicitly or implicitly an intention to repeat the misconduct.

(3) The applicant appears to be susceptible to blackmail.

(4) The misconduct involves:

(a) Open or public behavior;

(b) A person under the age of 18;

(c) Inducement of coercion by force or intimidation of another person;

(d) Prostitution;

(e) Sexual harrassment.

4. Mental or Emotional Illness. An abnormal mental condition that may cause a significant defect in the judgement or reliability of the individual concerned.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Conduct reflecting abnormal behavior indicative of mental illness even though there is no confirming medical history.

(2) Refusal by the individual concerned to furnish medical information or to allow medical information to be obtained for the purpose of determining the significance of bizarre behavior or conduct.

(3) Documented spouse or child abuse.

(4) Diagnosis by competent medical authority that an earlier incapacitating mental illness is of a type that has a high incidence of recurrence even though the individual concerned currently manifests no symptoms of mental or emotional illness.

5. Hostage and Foreign Connections. An applicant who has immediate family members or other persons to whom he or she is bonded by affection or obligattion residing in a communist country or other countries currently hostile to the United States. These countries are of two categories:

Category I - Countries which, based on current assessment of the U. S. Intelligence Community, possess an intelligence organization with a demonstrated capability of recruiting and exploiting U. S. personnel for intelligence purposes.

Category II - Countries which, although having national intelligence objectives inimical to the United States do not have the capability of exploiting U. S. personnel for intelligence purposes or have not undertaken to target U. S. personnel for such purposes.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Residence of a member of immediate family or a person to whom the individual is bound by affection or obligation in a Category I country.

(2) Travel, correspondence, or financial aid to Category I or Category II countries on a regular basis without satisfactory explanation.

(3) Dating or cohabiting with a foreign national from a Category I country.

6. Subversive Activity. Unlawfully advocating or practicing the commission of acts of force or violence to either prevent others from exercising their rights under the constitution or laws of the United States, or to overthrow or alter the form of Government of the United States by unconstitutional means. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons that support the above cited activities.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Organization is one which has been characterized by the Department of Justice as one which meets the above-cited criteria.

(2) Participation in acts that involve force or violence to prevent others from exercising their rights under the constitution or to overthrow or alter the form of Government of the United States.

(3) Monetary contributions, service, or other support of the organization with the intent of furthering the unlawful objectives of the organization.

(4) Deliberate misrepresentation of association with the organization.

(5) Evidence of continuing sympathy with the unlawful aims and objectives of the organization.

(6) Holding a position of major doctrinal or managerial influence in the organization.

7. Alcohol Abuse. The consumption of alcohol on an episodic or recurring basis that results in impairment of the individual's ability to perform assigned duties or to adequately safeguard classified information.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Use of alcohol which results in behavior that adversely affects a person's judgement, reliability or discretion.

(2) Repeated alcohol-related incidents.

(3) Alcohol consumption resulting in the deterioration of the individual's physical health, as determined by competent medical authority.

8. Drug Abuse. The illegal or improper use of any psychoactive substance to include any narcotic,[1] dangerous drug[2] or cannabis.[3]

a. Factors which may considered in determining whether to deny or revoke a clearance:

(1) Experimental abuse[4] of any narcotic or dangerous drug within the past 12 months.

(2) Occasional abuse[5] of any narcotic or dangerous drug within the last three years.

(3) Regular abuse[6] or addiction[7] to any narcotic or dangerous drug within the last five years.

(4) Regular abuse of cannabis within the last 12 months.

(5) Illegal trafficking, cultivation, processing, manufacture, sale, distribution or purchase of any narcotic, dangerous drug, or cannabis whether or not the individual was arrested for such activity.

(6) Information that the individual intends to continue to use (regardless of frequency) any narcotic, dangerous drug, or cannabis.

9. Security Violations. Failure to comply with policies and procedures established for the purpose of safeguarding classified information.

a. Factors which may be considered in determining whether to deny or revoke a clearance:

(1) Intentional disclosure of classified information to unauthorized persons.

FOOTNOTES FOR PARAGRAPH 8

1. Narcotic. Opium and opium derivatives or synthetic substitutes.

2. Dangerous Drug. Any of the non-narcotic drugs which are habit forming or have a potential for abuse because of their stimulant, depressant or hallucinogenic effect.

3. Cannabis. The intoxicating products of the hemp plant, cannabis sativa, including but not limited to marijuana, hashish, and hashish oil.

4. Experimental Abuse. Abuse occuring not more than a few times for reasons of curiosity, peer pressure, or other similar reasons.

5. Occasional Abuse. Recurrent, but infrequent abuse of drugs; no consistent pattern of drug abuse.

6. Regular Abuse. Drug abuse on a frequent recurrent basis to the point of habituation.

7. Addiction. Psychological or physical dependence to the point of compulsive use.

(1) Deliberate disregard of security regulations which results in the compromise of classified information.

(2) Recent deliberate violations of security regulations, such as, taking classified information home or carrying classified material while in a travel status without proper authorization.

(3) Nondeliberate security violations which indicate a pattern of negligence or carelessness.

0412. DENIAL/REVOCATION OF CLEARANCE

1. The authority to deny/revoke a security clearance of civilian personnel is vested in Naval Investigative Service Command (NISCOM). NISCOM reviews adverse information on civilian applicants for and employees in sensitive positions. Where there is reasonable doubt as to the individual's reliability and trustworthiness, NISCOM may refer the case material to the SPAWAR Security Office for further investigation or additional information.

2. The Security Office will evaluate all the derogatory information and is required to choose a course of action. Such action could include:

a. Reassigning the individual to a nonsensitive position.

b. Removing the individual on suitability grounds. The Security Office will coordinate suitability determinations with the supervisor concerned and the Central Civilian Personnel Office (CCPO).

c. Resubmitting the case to NISCOM with any additional information requested and recommendations on disposition of the case.

d. All letters of intent to deny/revoke clearance will be sent to the individual by NISCOM via the SPAWAR Security Office.

Section 2

SPECIAL ACCESS AUTHORIZATION

0413. GENERAL

1. Owing to their inherent sensitivity or international requirements, certain types of classified information require positive access/dissemination control measures. Therefore, the granting of access authorizations are rigidly controlled, kept to an absolute minimum consistent with efficient operations, and are requested only when a positive need exists and not for administrative convenience. Examples of types of information which require access authorization include, but are not limited to:

2. Single Integrated Operations Plan (SIOP) and Critical Nuclear Weapon Design Information (CNWDI). Access to SIOP and CNWDI requires the approval of SPAWAR 09. All requests for access are submitted to the Security Office furnishing name(s) and complete justification as to need.

3. Sensitive Compartmented Information (SCI). All requests for SCI access authorization are submitted to SPAWAR 00H in accordance with instructions issued by this office.

4. NATO. Access to NATO information is based on current security clearance at least equal to the classification of the NATO information involved, and a valid "need-to-know". When access is required, a written request shall be submitted to the Security Office signed at the Division level fully justifying the access required.

5. Cryptographic. Formal authorization for access to cryptographic material is no longer required. Access is based on "need-to-know" and an appropriate level of clearance.

0414. TERMINATING ACCESS AUTHORIZATIONS

Access authorizations will be terminated whenever the individual fails to meet any condition of eligibility. Requestors of the original access authorization are responsible for keeping the Security Office informed of all factors affecting continuation of access. The Security Office will ensure appropriate debriefings are administered and signed statements are obtained, as required.

EXHIBIT 4-1

MEMORANDUM

From:
To: SPAWAR 10H

Subj: SECURITY CLEARANCE REQUEST FOR _____ (EMPLOYEE NAME) _____

1. It is requested that subject employee be granted a _____ (Indicate Level) security clearance. This clearance is required in performance of the following specific duties:

2. I certify that the above duties cannot be performed without access to classified information at the degree indicated and that no other cleared personnel are available to perform these duties.

_____
(SIGNATURE)

NOTE: Top Secret Requests - Initiated by Deputy Commanders, Assistant Commanders, Program Directors and Heads of Staff Offices only.

Secret/Confidential Requests - Initiated by Division Directors or equivalent only.

CHAPTER V

CLASSIFICATION MANAGEMENT

Section 1

GENERAL

0501. CLASSIFICATION MANAGEMENT PROGRAM

1. Executive Order 12356 established new guidelines for the classification and declassification of official information in the interests of national security. The intent of the Executive Order is to ensure that information is appropriately classified and that classification is retained for the required periods of time.

2. The Security Office is assigned the responsibility and is designated the principal control office for administering the functions of the SPAWAR Classification Management Program. The Security Office will implement for SPAWAR the policies and procedures pertaining to classification, reclassification, declassification, and other applicable security directives.

0502. MISUSE OF CLASSIFICATION

Classification applies only to official information requiring protection in the interests of national security. It may not be used for the purpose of concealing administrative error or inefficiency, to prevent personal or departmental embarrassment, to influence competition or independent initiative, or to prevent release of official information which does not require protection in the interests of national security. Unnecessary classification and higher than necessary classification shall be scrupulously avoided.

Section 2

CLASSIFICATION CATEGORIES

0503. GENERAL

Official information which requires protection in the interests of national security is limited to three categories of classification which, in descending order of importance, carry one of the following designations: Top Secret, Secret, or Confidential. No other designation is used to classify defense

information, except as expressly provided by statute. The marking "For Official Use Only" and "Limited Official Use" are not classification markings and shall not be used to identify classified information.

0504. DEFINITION OF TOP SECRET

"Top Secret" is the designation which shall be applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

0505. DEFINITION OF SECRET

"Secret" is the designation which shall be applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

0506. DEFINTION OF CONFIDENTIAL

"Confidential" is the designation which shall be applied to information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. Examples of "damage" include the compromise of information which indicates strength or ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

0507. RESTRICTED DATA, FORMERLY RESTRICTED DATA, AND CNWDI

1. The term RESTRICTED DATA means all data concerning (a) the design, manufacture, or utilization of atomic weapons; (b) the production of special nuclear material; (c) the use of special nuclear material in the production of energy.

2. The term FORMERLY RESTRICTED DATA applies to that classified defense information removed from the RESTRICTED DATA category upon determination jointly by the Department of Energy and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information.

Such information is, however, treated the same as RESTRICTED DATA for purposes of foreign dissemination.

3. Critical Nuclear Weapon Design Information (CNWDI). Secret Restricted Data or Top Secret Restricted Data revealing the theory of operation of design of the components of a thermo-nuclear or implosion type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test or replace.

4. The requirements for protecting RESTRICTED DATA, FORMERLY RESTRICTED DATA, and CNWDI, are generally, the same as those for other material of the same classification.

0508. FOREIGN CLASSIFIED INFORMATION

1. To be identified as foreign government information, information must fall into one of the following two categories:

a. Information provided to the United States by a foreign government or international organization of Governments, such as the North Atlantic Treaty Organization (NATO), where the United States has undertaken an obligation, expressed or implied, to keep the information in confidence. The information is considered to have been provided in confidence if it is marked in a manner indicating it is to be treated in confidence or if the circumstances of the delivery indicates that the information is to be kept in confidence.

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

2. Classification

a. Foreign government information that is classified by a foreign entity shall either retain its original classification designation or be marked

with a United States classification designation that will ensure a degree of protection equivalent to that required by the entity that furnished the information. Original classification authority is not required for this purpose.

b. Foreign government information that was not classified by a foreign entity but was provided to the Department of the Navy with the expressed or implied obligation that it be held in confidence shall be classified. Such foreign government information shall be classified at least Confidential. However, at the time of classification, judicious consideration shall be given to the sensitivity of the subject matter and the impact of its unauthorized disclosure upon both the United States and the originating foreign government or organization of governments in order to determine the most appropriate level of classification. Levels above Confidential shall be assigned by an original classification authority.

Section 3

AUTHORITY TO CLASSIFY

0509. ORIGINAL CLASSIFICATION

1. Original classification is involved when an item of new information is developed which requires classification in the interest of the national security and when such classification cannot reasonably be derived from a previous classification still in force involving in substance the same, closely related or similar information. (See paragraph 2 for list of SPAWAR officials authorized to assign original classifications.)

2. Original classification authority is limited to those persons responsible for determining, from the defense standpoint, the security controls necessary to protect individual plans, programs or projects from their inception. Only the following personnel are authorized to assign original security classifications for SPAWAR and SPAWARSYSCOM field activities.

a. Top Secret. COMNAVSPAWAR is the only official in SPAWAR to whom such authority has been delegated. COMNAVSPAWAR is not authorized to delegate this authority or any other original classification authority. In the absence of an original classification authority, however, the person designated to act in his absence may exercise the classification authority.

b. Secret Those officials within SPAWAR to whom such authority has been delegated are:

Commander

Vice Commander

Assistant Commander, Acquisition and Logistics Planning (SPAWAR 003)

Director, Warfare Systems Architecture and Engineering (SPAWAR 30)

Program Director, Space and Sensor Systems (PD 40)

Program Director, Information Transfer Systems (PD 50)

Program Director, Information Management Systems (PD 60)

Program Director, Marine Corps Systems (PD 70)

Program Director, Anti-Submarine Warfare Systems (PD 80)

Holders of Secret authority are not authorized to delegate their authority or any other original classification authority. In the absence of the original classification authority, however, the person designated to act in his/her absence may exercise the classification authority.

c. Confidential. The Department of the Navy does not specifically designate original Confidential classification authorities. Those officials who hold Top Secret or Secret authority may exercise Confidential authority.

0510. DERIVATIVE CLASSIFICATION

1. Derivative classification is involved when:

a. Items of information are in substance the same as, or closely related to, other information with respect to which there is an outstanding proper classification determination, of which the classifier has knowledge and on which he is relying as his basis for classification; or

b. The information is created as a result of, in connection with or in response to other information dealing with substance with the same or closely related subject matter which has been and still is properly classified; or

c. The classification to be applied to the information has been determined previously by a higher authority and that determination is officially communicated to the classifier for implementation.

2. Derivative classification is the responsibility of each person whose official duties require decision by him/her as to whether information contained in or revealed by material he prepares or produces requires classification under the circumstances stated in subparagraph 1 above, subject to the following general rules:

a. The supervisor, or other official whose signature or other form of approval is required before a document or material may be issued, transmitted or referred outside the office of origin, is responsible for the necessity, currency and accuracy of the derivative classification assigned to that item.

b. Definite procedures shall be established by each SPAWAR office so that, without undue delay and as a matter of the regular course of business, the necessity, currency and accuracy of each derivative classification will be reviewed. When necessary, corrective action shall be taken or instituted.

3. In those situations involving the copying or extracting of classified information clearly identified in another document, or involving the reproduction or translation of a whole classified document, the individual responsible for such copying, extracting, reproduction or translation shall be responsible for assuring that the new document or copy bears the same classification as that assigned to the information or document from which the new document or copy was prepared.

0511. CLASSIFICATION PENDING

1. Safeguarding in the Absence of Authority to Classify

a. Nothing in this Chapter shall be construed to relieve originators or signature authorities of the responsibility to provide for adequate safeguarding of official information.

b. When a person originates or transmits material believed to require a classification that he is not authorized to assign, he/she shall recommend a classification by so marking it, state the reason, and refer the material to higher authority.

c. In respect to the foregoing, it is emphasized that, basically, a defense classification marking is merely a signal that the material so marked requires certain minimum controls and restrictions in respect to its accessibility. Should a person have occasion to observe, originate, forward, or disseminate material or information that in his/her best judgement requires a degree of safeguarding equivalent to that prescribed elsewhere in this manual for one of the three defense classifications, but who is not designated in paragraph 0509.2., he/she shall recommend classification, as appropriate, and provide adequate controls and precautions commensurate with the importance or sensitivity of such material or information in its handling and transmittal, to ensure against unauthorized or inadvertent disclosure.

2. Safeguarding during drafting or preparation

a. When material is under drafting or preparation for signature or classification by an official who has original classification authority, it is the responsibility of the person drafting or preparing the material to recommend a classification by so marking it in order that notes, discussions, and other pertinent material can be properly safeguarded.

Section 4

ORIGINAL CLASSIFICATION PRINCIPLES, CRITERIA AND CONSIDERATIONS

0512. JUDGEMENT REQUIREMENT

Original classification authorities must elect to classify when doubt exists as to whether or not classification is appropriate. In like fashion, the higher classification level must be selected when doubt exists as to which level of classification should be applied.

0513. IDENTIFICATION OF SPECIFIC INFORMATION

Classification determinations must be preceded by an exact identification of each item of information which may require security protection in the interests of national security. This process involves identification of that specific information which comprises the basis for the particular national advantage or advantages which, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting the national security.

0514. REASONS FOR CLASSIFICATION

An evaluation of information forms the base for classification. A document or other material is classified either because of the information it contains which may be ascertained by study, analysis, observation or use of it; or because of the information it may reveal when associated with other information, including that which the classifier knows already has been officially released into the public domain.

0515. SPECIFIC CLASSIFYING CRITERIA

A determination to classify shall be made only by an original classification authority and only when first, the information meets one or more of criteria in 1 through 8 below; and second, the unauthorized disclosure of the

information reasonably could be expected to cause damage to the national security. The determination involved in the first step is separate and distinct from that in the second. The fact that the information falls under one or more of the criteria shall not be presumed to mean that the information automatically meets the damage criteria. Information may not be considered for classification unless it concerns:

1. Military plans, weapons, or operations.

2. Foreign Government information.

3. Intelligence activities, sources or methods.

4. Foreign relations or foreign activities of the United States.

5. Scientific, technological, or economic matters relating to the national security. Specifically included are vulnerabilities and capabilities of systems, installations, projects and plans.

6. United States Government programs for safeguarding nuclear materials or facilities.

7. Cryptology.

8. Other categories of information which are related to national security and which require protection against unauthorized disclosures as determined by the Secretary of the Navy.

0516. CLASSIFYING RESEARCH DATA

Ordinarily, except for information which meets the definition of Restricted Data, basic scientific research or results thereof shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific "break-through," there is sound reason to believe it is now known or within the state-of-the-art of other nations, and it supplies the United States with an advantage directly related to national security.

0517. STATE-OF-THE-ART AND INTELLIGENCE

Classification requires consideration of the information available from intelligence source concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state-of-the-art in other nations is a vital factor requiring consideration.

Section 5

DURATION OF ORIGINAL CLASSIFICATION

0518. GENERAL

At the time a determination is made to originally classify information as Top Secret, Secret or Confidential, a simultaneous decision must be made as to the duration of time such classification shall remain in force. In arriving at the latter decision, the original classification authority shall exercise careful judgement as to how far in the future the basis for original classification remains valid.

0519. DURATION

1. The six and twenty-year declassification/review time limits of E. O. 12065 have been eliminated, which means that original classification authorities will now classify information for as long as required by national security considerations. If a specific date or event for downgrading or declassification can be determined, it should, of course, be used.

2. The mandatory twenty-year systematic review program has also been eliminated. The Archivist of the United States will, under the current Executive Order, systematically review for declassification all permanently valuable thirty-year old Navy records accessioned into the Archives pursuant to guidance provided by CNO (OP-09N).

Section 6

CLASSIFICATION GUIDANCE

0520. POLICY

1. A classification guide, based upon classification determinations made by original classification authorities, shall be promulgated for each system, plan, program or project involving classified information.

2. Classification Guides shall:

a. Identify the information elements to be protected, using categorization and subcategorization to the extent necessary to ensure that the information involved can be readily and uniformly identified.

b. State which of the classification designations, i.e., Top Secret, Secret, or Confidential apply to the identified information elements.

c. State the duration of each specified classification in terms of a period of time or future event, or that the originating agency will provide a declassification decision.

d. Indicate that the designations, time limits, markings and other requirements of Executive Order 12356 are to be applied to information, classified pursuant to the guide, in accordance with this regulation.

3. Each classification guide shall be approved personally and in writing by an official with appropriate original classification authority and cognizance over the material involved (See paragraph 0509 for such SPAWAR officials.)

0521. RETRIEVAL AND ANALYSIS OF NAVY CLASSIFIED INFORMATION (RANKIN)

1. Standard format, central recording and promulgation of Department of the Navy classification guidance shall be accomplished through the automated system designated as retrieval and analysis of Navy classified information (RANKIN). Through RANKIN, the Chief of Naval Operations (CNO) (OP-09N) shall provide standardization, a central data bank of information, central promulgation and timely updating of security classification guidance for Department of the Navy programs.

2. CNO (OP-09N) shall promulgate all Department of the Navy classification guides, separated into major subject categories, utilizing the OPNAVINST 5513 series as follows:

a. OPNAVINST 5513.1: Specific responsibilities for preparation, updating procedures and general administrative data.

b. OPNAVINST C5513.2: Air Warfare Guides.

c. OPNAVINST S5513.3: Surface Warfare Guides.

d. OPNAVINST S5513.4: Intelligence, Cover and Deception, and Investigative Guides.

e. OPNAVINST S5513.5: Undersea Warfare Guides.

f. OPNAVINST S5513.6: Communications and Satellites Guides.

g. OPNAVINST C5513.7: Mine Warfare Guides.

h. OPNAVINST S5513.8: Electronic Warfare Guides.

i. OPNAVINST S5513.9: Nuclear Warfare Guides.

j. OPNAVINST C5513.10: Miscellaneous Guides.

k. OPNAVINST 5513.11: Ground Combat Systems Guides.

l. OPNAVINST S5513.12: Intelligence Research Project Guides.

m. OPNAVINST S5513.13: Non-Acoustic ASW Guides.

3. The Security Office is responsible for administering the RANKIN system within SPAWAR and shall act as liaison between the Command and CNO (OP-09N). The Security Office will ensure that all SPAWAR systems, programs or projects including classified information have classification guides prepared in accordance with the procedures and format in OPNAVINST 5513.1.

4. SPAWAR codes are responsible for:

a. Preparing classification guides for each system, plan, program or project under their cognizance.

b. Conducting biennial reviews and making changes to existing guides.

c. Ensuring that all correspondence with CNO (OP-09N) relating to the RANKIN system, is coordinated with the Security Office.

Section 7

MARKING REQUIREMENTS

0522. GENERAL

1. Originally Classified Documents. At the time of original classification, the following shall be shown on the face of paper copies of originally classified documents:

a. The identifier of the original classification authority unless that authority is also the signer or approving authority.

b. The date of origin.

c. The office of origin.

d. The overall classification of the document.

e. The declassification date or event or the notation "Originating Agency's Determination Required" or "OADR."

f. If appropriate, date and downgrading action to be taken.

2. Derivatively Classified Documents. At the time of origin, paper copies of derivatively classified documents shall show on their face:

a. The source of classification (e.g., source document or classification guide). If classification is derived from more than one source, the phrase "Multiple Sources" shall be shown.

b. The date of origin.

c. The office of origin.

d. The overall classification of the document.

e. The date for declassification or the notation "Originating Agency's Determination Required" or "OADR."

f. If appropriate, date and downgrading action to be taken.

g. Any additional warning notices.

3. In addition to the foregoing, any appropriate special warning notices will be shown on the face of the document. Such notations will be carried forward from source documents to derivatively classified material when appropriate.

4. Material other than documents shall, to the extent practical, show the foregoing on the material itself or in related or accompanying documentation.

0523. OVERALL AND PAGE MARKING

The overall classification of a document shall be marked, stamped or permanently affixed at the top and bottom of the outside of 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), classification markings 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. To achieve production efficiency, each interior page of a classified document normally shall be marked or stamped at the top and bottom according to the highest overall classification of the document.

0524. MARKING COMPONENTS

Major components of some documents are likely to be used separately. In such instances, each major component shall be marked as a separate document. Examples include each annex, appendix, or similar component of a plan, program or operations order; attachments and appendices to a memorandum or letter; or each chapter of a report or document.

0525. PORTION AND PARAGRAPH MARKINGS

1. Each portion, section, part, paragraph or subparagraph of a classified document shall be marked to show the level of classification, or that the portion, section, part, paragraph or subparagraph is unclassified. It is the intent of this requirement that a document and portions of a document be sufficiently well marked that any uncertainty as to which of its portions contains or reveals information which must be protected will have been eliminated. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion or number, or in the absence of letters or numbers, immediately before the beginning of the portion. The parenthetical symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified, shall be used. When appropriate, the symbols "RD" for Restricted Data and "FRD" for Formerly Restricted Data shall be added, e.g., "(S-RD)" or "(C-FRD)."

2. Except in those cases where a source of intelligence would be revealed, portions, sections, parts, paragraphs or subparagraphs of United States documents containing foreign government information shall be marked to reflect the country or international organization of origin as well as the appropriate classification, e.g., "(NATO-S)" or "(U. K.-C)." Such documents will also bear the notation "This Document Contains Foreign Government (or NATO classified) Information" on their face.

3. The classification of the text of the lead-in portion of a subparagraph will be indicated at the beginning of the text with the appropriate parenthetical symbol. The classification of subordinate portions or subparagraphs shall be shown by the appropriate parenthetical symbol immediately following the portion letter or number. In the absence of letters or numbers, classification shall be shown immediately before the beginning of the paragraph or subparagraph. (See Exhibit 5-1.)

4. If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the classified document shall contain a description on its face sufficient to identify the exact information that is classified and the classification levels assigned.

0526. COMPILATIONS

In cases where the use of classification is required to protect a compilation of information, in addition to the markings required by this chapter, the face of the document shall include a statement containing the following elements: The fact that the individual parts are unclassified or of a lower classification; and the reason the compilation warrants classification or a higher classification.

0527. SUBJECTS AND TITLES

Subjects and titles shall be selected, if possible, so as not to require classification. A classified subject or title may be used, however, when necessary to convey meaning. In that case, an unclassified short title shall be added for status, a subject or title shall be marked with the appropriate parenthetical symbol placed immediately following.

0528. FILE, FOLDER, OR GROUP OF DOCUMENTS

Files, folders or groups of documents shall be conspicuosly marked to ensure their protection to a degree as high as that of the most highly classified document included. Classified document cover sheets may be used for this purpose. Documents separated from the file, folder or group shall be marked as prescribed for individual documents.

0529. TRANSMITTAL DOCUMENTS

A transmittal document or endorsement added to basic correspondence shall carry on its face a notation as to the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document or endorsement standing alone. For example, an unclassified document which transmits a classified document as an enclosure, shall bear a notation as follows: "Unclassified Upon Removal of Enclosures."

0530. ELECTRICALLY TRANSMITTED MESSAGES

The from line of a message will serve as the "classified by" line. Other parts of the downgrading/declassification notations are included on the last line of the text in abbreviated form. For example, the last line of a message would read: "DECL: 6 Jun 98."

0531. CLASSIFICATION MARKINGS ON SPECIAL TYPES OF MATERIAL

1. General Provisions. The security classification, designation, downgrading (if any) and declassification instructions shall be conspicuously stamped, printed, written, painted or affixed by means of a tag, sticker,

decal, or similar device on classified material other than documents, and on their containers, if possible. If the material or container cannot be marked, written notification of the security classification shall be furnished to recipients.

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

3. Photographs. Negatives and positives shall be marked with the appropriate classification markings and kept in containers bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip and single negatives marked with the appropriate classification. Caution must be exercised when using self-processing film or paper to photograph or reduce classified material, since the negative of the last exposure may remain in the camera. All components parts of the last exposure shall be removed and destroyed as classified waste or the camera shall be protected as classified material. All prints, 8" X 10" or larger, shall be marked top and bottom on the reverse side with the appropriate classification, with the downgrading and declassification instructions at the bottom. The classification marking need be applied only once on smaller prints. The marking shall appear on the face side whenever practicable. In any case, at least the classification must be shown on the face side and may be affixed by pressure tape label or stapled strip if a stamp could not be used. All separate reproductions of the photograph will show the classification and declassification markings.

4. Transparencies and Slides. Whenever possible, the applicable classification markings shall be shown clearly on the image of each transparency or slide. If, in special circumstances, the classification markings cannot be shown on the transparency or slide, they shall be shown on its border, holder, or frame. When transparencies or slides are reproduced as part of hard copy text material, abbreviated downgrading and declassification marking shall show below the classification marking on the image.

5. Decks of Accounting Machine Punched or Aperture Cards A deck of classified accounting machine punched or aperture cards shall be marked as a single document. Only the first and last card require classification markings. A deck so marked shall be stored, transmitted, destroyed and otherwise handled in the manner prescribed for other classified documents of the same classification. An additional card shall be added (or the job control card modified),

however, to identify the contents of the deck (at a minimum, the number of cards) and the highest classification involved. Alternatively, a manual log for decks undergoing frequent change may be employed. Cards removed for separate processing or use, and not immediately returned to the deck after processing or use shall be protected to prevent compromise of any classified information they contain, and for this purpose shall be marked individually as prescribed for an individual, ordinary document.

6. Computer and Automated Information System (AIS). Removable magnetic media generated by computer and AIS shall bear external markings and internal notations sufficient to assure that any recipient of the tapes, or of the classified information they contain when reproduced by any medium, will know that classified information of a specific classification category is involved.

7. Documents Produced by Computer and Automated Information Systems (AIS). At a minimum, the first page, and the front and back covers, if any, of documents produced by computers and AIS shall be marked as prescribed in paragraph 0523. Classification markings of interior pages may be applied by the computer and AIS equipment or by other means. When the application by the computer and AIS, of declassification instructions and other markings prescribed by paragraph 0522 is not consistent with economic and efficient use of such equipment, such instructions and markings may be applied to a document produced by superimposing upon the first page of such document a "Notice of Declassification Instructions and Other Associated Markings." Such notice shall include the date or event for declassification and all other such applicable markings. If individual pages of a document produced by computer and AIS are removed or reproduced for distribution to other users, each such page or group of pages shall be marked as prescribed in paragraph 0523 or by superimposing on each page or group of pages, a copy of any "Notice of Declassification Instructions and Other Associated Markings" applicable to such page or group of pages.

Section 8

DOWNGRADING, DECLASSIFICATION OR UPGRADING

0532. POLICY

Whenever classified information is downgraded, declassified, or upgraded, the material containing the classified information shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and identity of person taking the action. In addition, the old classification markings shall be cancelled, if practicable, but in any event those on the first page, and the new classification markings (or "Un-

classified" if appropriate) shall be substituted. When classified information is downgraded or declassified under the provisions of this regulation and is marked in advance for downgrading or declassification, such markings shall suffice to meet the aforementioned authority notation.

0533. CONVERTING OLD DOWNGRADING/DECLASSIFICATION MARKINGS TO NEWLY CREATED INFORMATION OR MATERIAL

1. If a source document contains a specific date or event for declassification, then that date is carried forward.

2. If a source document contains a date for declassification review, then the notation "Originating Agency's Determination Required" or "OADR" is used.

0534. REMARKING DOCUMENTS AND MATERIAL ORIGINATED PRIOR TO 1 AUGUST 1982

There is no need to remark documents marked under E. O. 12065 or predecessor orders. Those already marked with specific date or event for downgrading or declassification will be downgraded or declassified accordingly. Documents not marked for automatic downgrading or declassification on a specific date or event will not be downgraded or declassified without authorization of the originating agency. Information extracted from such documents shall be marked "Originating Agency's Determination Required" or in the abbreviated form "OADR."

0535. RESTRICTED DATA AND FORMERLY RESTRICTED DATA

The RESTRICTED DATA and FORMERLY RESTRICTED DATA markings (see paragraph 0537) are, in themselves, evidence of extended classification. Except for electrically transmitted messages, only a "Classified by" line shall be added above the RD or FRD warning notice.

Section 9

WARNING NOTICES

0536. GENERAL

When applicable, one or more of the following warning notices shall be prominently displayed on classified documents or materials in addition to the foregoing marking requirements. On documents, these warning notices shall be conspicuously marked on the outside of the front cover or the first page if there is no front cover. When display of warning notices on other materials is not feasible, the warnings shall be included in the written notification of the assigned classification.

0537. RESTRICTED DATA AND FORMERLY RESTRICTED DATA

For classified information containing Restricted Data or Formerly Restricted Data, as defined in the Atomic Energy Act of 1954 as amended, those markings prescribed by the Department of Energy are to be applied:

1. RESTRICTED DATA. "This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative sanctions."

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

0538. DISSEMINATION AND REPRODUCTION NOTICE

For classified information which the originator has determined is subject to special dissemination and reproduction limitations, statements as follows shall be shown:

1. "Reproduction requires approval of originator or higher DoD authority."

2. "Further dissemination only as directed by (insert appropriate activity or official) or higher DoD authority."

Reproduction of all or portions of the information contained in documents marked under 1 is prohibited without authority of the originating office or higher authority. Dissemination of all or portions of the information contained in documents marked under 2 is prohibited without authority of the designated activity or official.

0539. INTELLIGENCE SOURCES AND METHODS INFORMATION

For classified information on intelligence sources and methods, the following warning notice shall be used:

"Warning Notice - Intelligence sources or methods involved."

0540. NAVAL NUCLEAR PROPULSION INFORMATION

In light of the national policy on foreign disclosure of naval nuclear propulsion information, one of the following special warning notices may be used on document containing classified or unclassified naval nuclear propulsion information:

"Special Handing Required - Not Releasable to Foreign Nationals."

"NOFORN"

"This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the (Originating Command)."

0541. COMSEC MATERIAL

COMSEC documents, prior to being released to contractors, will contain on the title page, or first page if no title page exists, the notation, "COMSEC Material - Access by contractor personnel restricted to U. S. citizens holding final Government clearance." This notation should be placed on COMSEC documents at the time of their publication when release to contractors can be anticipated. Other COMSEC material shall be marked in accordance with National COMSEC Instruction (NACSI) 4005. Foreign dissemination of COMSEC information is controlled by the Security Office.

0542. NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)

1. The marking, "Not Releasable to Foreign Nationals," may be used only on documents containing foreign intelligence material and naval nuclear propulsion information.

2. The abbreviation NOFORN is authorized for the information described above when used in electrically transmitted messages, automatic data processing and paragraph marking.

3. The marking, "No Foreign Dissem", is no longer authorized.

EXHIBIT 5-1

EXAMPLE MARKING LETTER

SECRET

From: Commander, Space and Naval Warfare Systems Command
To: Commander, Naval Sea Systems Command

Subj: SECURITY CLASSIFICATION OF THE SUBJECT FOLLOWS IT (U)

1. (C) The classification of the lead-in portion of a paragraph follows the pargaraph number. For example, this lead-in portion is CONFIDENTIAL and is marked as shown, even though subsequent subparagraphs are SECRET.

a. (S) The same rule extends to subparagraphs. Each subdivision of a paragraph carries only its own classification, following the subdivision designation.

b. (U) Therefore, the classification following a paragraph designation does not indicate the overall classification of the paragraph and its subdivisions.

(1) (C) Subparagraphs and additional subdivisions are marked for their content.

(2) (C) Marking of subparagraphs and subdivisions is required even when they are all the same classification.

c. (C) Subdivisions need not be marked if they don't express a complete thought. For example, subdivisions would not be marked if they were a list of components:

(1) Top with stripe.
(2) Wiring board.
(3) Metal box.

CLASSIFIED BY: OPNAVINST 5513.8-10
DECLASSIFY ON OADR

Note: Secret for training, otherwise unclassified

SECRET

EXHIBIT 5-1 (Cont'd)

SECRET

2. (U) When a paragraph or subparagraph is unclassified, its subdivisions need not be marked if they are also unclassified.

a. Downgrading and declassification markings shall be placed at the lower left of the page and only appear on the first page of the letter.

b. The RESTRICTED or FORMERLY RESTRICTED caveat shall be typed after the classification. The full marking is placed at the lower right. Other warning notices shall be typed following the classification at the top.

c. The marking requirement for military memorandum and business type letters are identical to those of a military letter.

3. (U) The from line of a message will serve as the "Classified by" line. Other parts of the downgrading/declassification notations are included on the last line of the text in abbreviated form. For example, the last line of a message would read "DECL: 6JUN98."

Note: SECRET for training, otherwise unclassified.

SECRET

CHAPTER VI

FOREIGN DISCLOSURES

Section 1

RELEASE OF DOCUMENTARY INFORMATION

0601. HEADQUARTERS

1. Classified Information. No classified information shall be disclosed to foreign nationals without the specific approval of the Security Office.

2. Unclassified Information

a. Foreign Government Request. Unclassified information may be released to friendly foreign governments after review by the Security Office providing the following criteria are met.

(1) The information is in all respects releasable to the Government of the recipient country.

(2) The recipient country is considered to have a reasonable need for the information in support of military programs.

(3) Documents and reports have been reviewed, and all references, if any, to classified publications, programs, etc., have been removed. (Exception to this requirement is permitted if it is known that all references would be or have been released to the recipient country.)

(4) All transmittals to be on a "Government-to-Government basis.

b. Non-Government Requests. The Security Office will prepare responses to all non-Government requests or provide specific response guidance on a case-by-case basis.

3. Procedures

a. All foreign requests for documentary information received within Headquarters by any individual or organizational entity will be forwarded to SPAWAR 18-51 for recording and routing to the Security Office.

b. The Security Office will develop eligibility and disclosure criteria and will solicit specific comments and recommendations from the cognizant codes involved. Codes having primary cognizance over the information requested shall obtain the necessary documentation and forward to the Security Office with comments and/or recommendations regarding releasability.

4. Foreign Requests for Participation in SPAWAR Procurements

a. All foreign contractor requests to compete for, or to participate in, Department of Navy contracts must be carefully reviewed to determine at the outset any requirement for the disclosure of U. S. classified information or unclassified information containing critical technology with military or space application during the entire program cycle.

b. In order to ensure applicable disclosure policies and restrictions are fully considered, SPAWAR contract and/or procurement representatives shall submit to SPAWAR 10H, by memorandum, the following information:

(1) Identification of the foreign source.

(2) The extent of that foreign source's expected involvement in the procurement effort.

(3) A detailed listing of classified information or unclassified information containing critical technology required for bid purposes and throughout the life of the contract.

(4) Any requirements for the foreign source to visit other commands, shipyards, fleet units, other contractors or Government activities.

(5) Any requirements to attend general meetings, conferences/symposia prior to bid, if unknown, so state.

c. SPAWAR 10H will evaluate the foreign source's involvement and forward to Naval Office of Technology Transfer and Security Assistance (NAVOTTSA) for a decision.

d. Proposal to exclude foreign contractors from procurement program and/or bidders conferences must also be referred to SPAWAR 10H. The final decision (i.e., approval or denial) will be provided by NAVOTTSA.

0602. SPAWAR ACTIVITIES

1. Classified Information. Disclosure of classified information is prohibited unless approved by SPAWAR 10H, NAVOTTSA or under the provisions of a Navy approved international exchange agreement/MOU, etc. OPNAVINST 5510.48 (series) provides policy and guidance. All approved disclosures must be accomplished on a government-to-government basis and marked with appropriate conditions of release.

2. Unclassified Information

a. Government Requesters. Unclassified information may be provided to allied and friendly government requesters without reference to SPAWAR Headquarters, subject to compliance with criteria of paragraph 0601.2a above.

b. Non-Government Requesters. Requests from allied and friendly country organizations or persons not representing their government for information not approved for public release shall be denied. Such requests should be returned indicating the U. S. Navy releases information only on a government-to-government basis for military purposes. Unclassified information approved for public release may be provided if there is reasonable assurance that the request is bona fide and could result in a "quid-pro-quo" arrangement.

3. Communist and Hostile Country Requests. Requests from communist and hostile controlled countries for publicly released material should normally be denied or referred to the National Technical Information Service. Should circumstances exist that may warrant an exception to these procedures, the request and supporting justification should be forwarded to SPAWAR 10H for decision on a case-by-case basis. A minimum of 30 days should be allowed for review.

4. Foreign Contracting. Approval to contract with foreign firms involving access to classified or unclassified critical technology with military or space application shall be submitted to NAVOTTSA via SPAWAR 10H forwarding the information required by paragraph 0601.4. Proposals to deny foreign contractors requests to participate shall be processed in the same manner providing rationale for such action.

5. Procedures. Commanders will establish a review system to ensure that the provisions of this Chapter are fully complied with. The system shall include:

a. A record of all releases to include a description of the material released, identification of the requestor and date of release.

b. A record of what information was received in the "quid-pro-quo" arrangement.

This review process shall be made available for inspection during SPAWAR Headquarters oversight visits.

Section 2

OFFICIAL VISITS ABROAD

0603. DEFINITION

Visits abroad involve official contact with foreign nationals for the purpose of disclosure or obtaining information. It does not include visits to U. S. military installations or ships located abroad when exchange of information with foreign nationals is not required. Visits abroad conducted under Information Exchange Projects (IEPS) and Mutual Weapons Development Data Exchange Agreements (MWDDEAS) are governed by the requirements and procedures established by individual agreements (see Section 5 of this chapter). Visits not involving official contact with foreign nationals are subject to the provisions of OPNAVINST 4650.11 (current series).

0604. GENERAL

Disclosure of classified information to foreign governments is premised on the basis that its disclosure will result in a net advantage to the United States and is otherwise releasable in accordance with the overall national policy toward the recipient country. Accordingly, requests to make classified disclosures in the performance of official travel abroad shall only be initiated when a net advantage to the interest of the United States is clearly apparent. Authorization from the Security Office is not required for unclassified disclosures if essential to the successful accomplishment of the visit and conforming to the criteria of paragraph 0601.2.

0605. PROCEDURES

1. Requesting Disclosure Authorization

a. When it is deemed essential for the accomplishment of official travel abroad to disclose classified information to foreign recipients, SPAWAR codes and field activities, as appropriate, shall submit their request to the SPAWAR Security Office 45 days in advance of visit furnishing the following information:

(1) Full name(s) of traveler(s).

(2) Summary and classification of information to be disclosed in sufficient detail to permit a foreign release determination.

(3) Specific Government and/or industrial organizations to whom disclosures will be made.

(4) Dates of visits.

(5) Advantages or benefits accruing to the United States as a result of the proposed disclosure.

b. The Security Office, after assuring releasability of the proposed disclosure based on all available release guidance and SPAWAR internal release policies, will request disclosure authority from NAVOTTSA. After receipt of the official U. S. Navy release decision, the SPAWAR Security Office will notify the requester of this decision along with any release limitations or other security considerations that may be required.

2. Visit Notification, Special Briefing and Reports

a. After receipt of disclosure approval, SPAWAR offices and field activities, as appropriate, shall concurrently request area/country clearance from the cognizant overseas area commander as listed by OPNAVINST 4650.11 (current series) and provide advance visit notification to the cognizant U. S. Defense Attache, furnishing the following information:

(1) Full name(s) of traveler(s) and activity or organization associated with, if other than the originator of the letter or message.

(2) Date and place of birth.

(3) Title and rank.

(4) Home address.

(5) Degree of security clearance and basis.

(6) Identification (passport, military I. D. card, building pass number, etc.).

(7) Activities to be visited and persons to be contacted, if known.

(8) Specific date(s) of visit(s)

(9) Purpose of visit in sufficient detail to permit necessary arrangements to be made.

(10) Foreign language capability (when visiting non-English speaking countries).

(11) Indicate whether or not disclosure of U. S. classified information has been authorized and/or required. If classified U. S. disclosures are authorized, indicate authority as well as classification and release restrictions imposed (see paragraph 1b above).

(12) Estimated time of arrival, flight number, etc.

(13) Whether or not travel or hotel assistance is required.

b. Visit notification shall be sent sufficiently in advance of the visit to permit the necessary arrangments to be made. OPNAVINST 4650.11 (current series) outlines lead time requirements for certain countries. Visit notification for all other countries shall be sent at least 30 days prior to the actual visit. Information copies of the visit notification shall be provided as follows:

(1) Navy Office of Technology Transfer and Security Assistance (NAVOTTSA)

(2) Commander, Task Force 168.

(3) SPAWAR Security Office.

(4) Any other activity concerned or having interest.

c. Security Briefing. Paragraph 3-11.1A of reference (a), obtainable from SPAWAR 10H, outlines security precautions applicable to travel in all foreign areas. All travelers shall familiarize themselves with this directive and ensure total compliance. Additional security briefings for Headquarters personnel will be administered by the Security Office as required.

d. Foreign Visit Report. Immediately upon completion of the visit the traveler shall submit a report of the visit including the following:

(1) Foreign activities visited and important contacts made.

(2) A brief account of information acquired.

(3) A brief account of information disclosed.

(4) If applicable, the subjects of detailed reports to be written by the traveler as a result of the visit.

Copies of this report shall be disseminated to the Security Office, Commander, Naval Intelligence Command, and the Defense Attache Office (DAO) of the country(s) visited.

e. Visit Appointments. Travelers shall make specific visit appointments with foreign officials/representatives only through the appropriate U. S. Defense Attache. However, such appointments may be made through other channels if it is known that it would more readily facilitate the traveler's objectives. In these circumstances the Defense Attache should be informed of the facts prior to the visit.

f. Cancellation of Visit. In the event it becomes necessary to cancel or postpone a visit for which notification has been made to the cognizant Attache, and appointments with foreign nationals have been made, the traveler shall ensure that the cognizant Attache is notified, by message, giving copies to recipients of original notification.

g. Reporting. Upon arrival in a foreign country, the traveler is required to report to the U. S. Defense Attache Office. If unable to report in person, the traveler shall use some other appropriate means of communication.

0606. VISITS TO THE U. S. S. R. AND BLOC COUNTRIES

OPNAVINST 4650.11 (current series) outlines various requirements with regard to travel to or through the U. S. S. R and Bloc countries, regardless of whether or not technical disclosures or official contact with foreign nationals are required (includes non-Government related travel). The Security Office is assigned responsibility for ensuring full compliance with these requirements, both for Headquarters and field personnel. All requests to visit Soviet and Bloc countries shall be forwarded to the Security Office for approval. Requests must outline in detail the purpose of the visit and furnish all pertinent information, such as copies of invitations, announcements, etc. This requirement is also applicable to attendance at international conferences, meetings, etc., regardless of location, including the United States, when it is known or can be anticipated that Communist country representatives will be in attendance. If visit is approved, the Security Office will furnish the traveler or SPAWARSYSCOM field activity with the name and address of the agencies/commands that must be notified and provide for any security briefing and debriefing required. (Field activities need send only official travel requests to Headquarters for approval, personal travel may be approved locally).

Section 3

LOCAL FOREIGN VISITS

0607. PROCEDURES

The following procedures are established to control disclosures of information to foreign nationals through local visits.

1. Visits to Headquarters

a. SPAWAR officials expecting a visit from a foreign national will:

(1) Notify SPAWAR 10H (by telephone or memo) at least two (2) working days prior to the visit (if SPAWAR 10H receives this notification from the foreign source, it will be confirmed with SPAWAR official being visited).

(2) Only accept foreign visitors if there is a reasonable expectation of a benefit to SPAWAR resulting from the visit.

(3) Only discuss information approved for release in the Foreign Visit Authorization Form (SPAWAR 5512/6) (Exhibit 6-1).

(4) Obtain Part I of the Visit Authorization Form from the visitor upon arrival. When the visit has been completed, fill out Part II of the form and return both parts to SPAWAR 10H by the end of the working day following the visit.

NOTE 1: The disclosure restrictions listed in Part II of the form shall not be imparted to the visitor.

NOTE 2: Classified documents shall not be released to foreign nationals during the course of a visit. Unclassified documents relating to the approved visit may be released directly to the visitor(s) provided they conform to the policy constraints established in Section 1 of this chapter. Identification of all documents released shall be included in Part II of the authorization form.

b. Upon receipt of notification of a foreign visit, SPAWAR 10H will:

(1) Review the request for compliance with this instruction.

(2) If the request is in compliance, prepare a Foreign Visit Authorization Form (SPAWAR 5512/6) (Exhibit 6-1).

(3) Provide Part I of this form to the Visitor Control Office for signature and pick-up by the visitor(s).

(4) Provide the SPAWAR official being visited with Part II of the authorization form.

(5) Review and retain the completed authorization form following the visit.

2. Visits to Local Foreign Entities. SPAWAR personnel visiting local foreign entities will obtain the approval of the Security Office at least 48 hours prior to the visit. A memorandum, containing the information outlined by Exhibit 6-2, signed at the Division level or higher, shall be used to obtain the Security Office approval. The reverse side of Exhibit 6-2 shall be completed and returned to the Security Office by the next working day following the visit.

3. Visits to SPAWAR Activities

a. Activities will receive tasking from, and respond directly to, the Naval Office of Technology Transfer and Security Assistance (NAVOTTSA) for visits by foreign nationals. Recommendations made by the activities concerning such visits will be returned to NAVOTTSA via the cognizant sponsoring activity (NAVSEA, NAVAIR, etc.) with an information copy to SPAWAR 10H. Disclosures made during such visits will be limited to the specific terms and conditions of the NAVOTTSA authorization.

b. SPAWARSYSCOM field activities may approve unclassified visits by representatives of friendly foreign Governments to their activities provided disclosures can effectively be limited to unclassified and provided the unclassified disclosure criteria established herein have been met.

4. Special Reports. Should any foreign national express undue interest in information which he is not authorized to receive, or if any irregular behavior or action by foreign nationals is observed, advise the Security Office immediately. Security violations and incidents involving unauthorized access by foreign nationals shall be documented and reported expeditiously to the Security Office for appropriate action.

Section 4

INTERNATIONAL INFORMATION EXCHANGE AGREEMENTS

0608. BACKGROUND

1. The purpose of the International Information Exchange Agreements is to bring about an exchange of scientific and technical information between the U. S. and allied and friendly nations. It is the principal means by which the U. S. Navy keeps abreast of foreign technology to improve the U. S. Navy technology base, eliminate costly and duplicative R&D, achieve standardization and interoperability of equipment, and promote closer ties with allied and friendly nations. Thus, it is important that military developments abroad be carefully observed. When it is in our interest to exchange needed technology

on a reciprocal basis, the U. S. Navy has entered into formal information exchange programs. Essentially the Navy participates in two types of programs, the U. S. Navy Information Exchange Project (IEP) and Mutual Weapons Development Data Exchange Agreement (MWDDEA). The IEPS are usually broader in scope and include operational, test and procedural matters. These IEPS may be multinational and involve exchange of information of a higher classification with selected foreign Governments. MWDDEAs are bilateral in nature and are primarily concerned with subjects of a technical nature and allow for the exchange of R&D information only in usually a narrow focused technology area.

2. Four important factors are to be considered prior to the establishing of and/or participating in, IEPs and MWDDEAs:

a. The current policy of the U. S. toward military cooperation with the participating country in the areas proposed.

b. Will sufficient benefits to the interest of the U. S. accrue.

c. The security capability of the foreign country to safeguard the classified information it may receive is adequate.

d. The information involved is in all respects releasable to the country concerned.

3. To ensure that all these factors are carefully considered and evaluated, the responsibility for coordinating the establishment and/or permitting participation in international exchange agreements is assigned to the Security Office with the International Programs Office providing supporting technology transfer and International Programs policy inputs and the Command technical offices providing technical and program inputs as required.

0609 POLICY

The Command in support of Department of the Navy and within the security considerations of this chapter will:

a. Promote cooperation with Allied and friendly nations in the research, development, test, evaluation, acquisition and logistics support of military systems;

b. Exchange needed technology with Allied and friendly nations on a reciprocal basis to satisfy mutual R&D requirements; and

c. Maximize the benefits of cooperation programs for developing the data base and criteria for controlling the export of U. S. and Western critical technology and end products.

0610. DISCLOSURE OF CLASSIFIED INFORMATION

Section 1 of this chapter states that no classified information shall be disclosed to foreign nationals without the specific approval of the Security Office. Once an IEP or MWDDEA has been approved and properly executed, authority for approving disclosures pursuant thereto is delegated to the project officer or participant. All disclosures and visit arrangements shall be in accordance with the provisions of the particular agreement involved. (Note: Visits to this Command are still subject to the provisions of Section 3 of this chapter.)

0611. ESTABLISHING AND/OR PARTICIPATING IN EXCHANGE AGREEMENTS

1. When it is determined that a need exists for the establishment of an information exchange agreement or participation in an existing agreement, a written request shall be submitted to the Security Office via the cognizant Deputy Commander (or equivalent) and the International Programs Office furnishing the following information:

a. Specific justifications, i.e., why required, what benefits will accrue to the U. S., etc.

b. Title and technical scope of the proposed agreement.

c. Highest security classification of information to be exchanged.

d. U. S. and foreign activities recommended for participation.

e. Recommended U. S. project office assignment, name, title and rank.

f. A proposed U. S. EYES ONLY annex outlining release restrictions.

2. The Security Office after assuring releasability of the information proposed for exchange and compliance with national and Command disclosure policies, will initiate a request to the Chief of Naval Operations requesting establishment of the recommended agreement.

0612. RESPONSIBILITIES

1. The project officer is responsible for overall administration of the agreement and for:

a. Assuring that all visits and documentary releases are limited to listed participants.

b. Assuring that all classified disclosures are clearly within the scope and classification limits of the agreement, and in all respects releasable.

c. Maintaining separate records of all classified disclosures and other transactions pertinent to the project.

d. Prepare trip reports for every DEA visit and an annual report for each DEA citing the information exchanged, the value of the information/technology received and the merits of continuing the exchange.

2. The International Programs Office will provide technical and IP assessments for compliance with International and U. S. Navy IP policy.

3. The Security Office will provide security policy and procedural guidance, as required. In addition, they will periodically review for compliance with security regulations.

0613. SCIENTIST AND ENGINEER EXCHANGE PROGRAMS

1. The purpose of Navy Scientist and Engineer Exchange Programs is to bring about an exchange of scientific and technical information between the U. S. and allied and friendly nations. It is a principal means by which the U. S. Navy keeps abreast of foreign technology to improve the U. S. Navy technology base, eliminates costly and duplicative R&D, achieves standardization and interoperability of equipment, and promotes closer ties with allied and friendly nations. Thus, it is important that military developments abroad be carefully observed. Paragraph 20410 of OPNAVINST 5510.48J provides details of this program.

2. Four important factors are to be considered prior to establishing an exchange scientist/engineer billet are as indicated in paragraph 0608.2 above.

3. To ensure that all these factors are carefully considered and evaluated, the responsibility for coordinating the establishment and/or permitting participation in, these exchange programs is assigned to the Security Office (SPAWAR 10H). Requests for participation should be forwarded to SPAWAR 10H and address:

a. Specific justification for participation.

b. Specific benefits that would be realized by the U. S. Navy and SPAWAR.

c. Technical scope of tasks to be performed.

d. Classification of information involved.

e. Specific protective measures to be taken to ensure no unauthorized disclosures occur.

f. Travel requirements for participating person(s).

g. Sponsor concurrence when assignment involves exposure to non-SPAWAR sponsored tasks.

4. No commitments should be made to foreign personnel regarding assignment until you receive approval of your request.

SECTION 5

NATO SECURITY PROCEDURES

0614. GENERAL

1. These procedures are designed to protect NATO classified information and material in accordance with the policy established by the United States Security Authority (USSA) for NATO affairs. "NATO" is a marking which signifies that a document is the property of the North Atlantic Treaty Organization (NATO). To control the dissemination of NATO information within the United States, the Central U. S. Registry has established NATO Subregisteries at major activities. It is the responsibility of these NATO Subregisteries to establish control points for the distribution and control of NATO information. A U. S. NATO Secret Subregistry has been established for SPAWAR. Control point in SPAWAR for the control and dissemination of NATO material is SPAWAR 18-512.

2. The NATO Control Officer appointed for SPAWAR is the Director, Security Office, and alternate Control Officer is SPAWAR 18-512. Detailed instructions for control points outside of the SPAWAR Subregistry may be found in SPAWAR Instruction 5510.22. SPAWAR 18-512 will maintain a log that will identify all NATO Secret documents received, their distribution and disposition. NATO Confidential and below will be destroyed by the local custodian when no longer needed. A log is not required.

0615. DEFINITIONS OF TERMS

1. NATO. The word "NATO" signifies that the document is the property of North Atlantic Treaty Organization (NATO) and is subject to access by any member nation under the special security procedures governing such information. *"NATO" markings are applied only to Secret, Confidential, Restricted and* Unclassified documents accepted for circulation within NATO.

2. ATOMAL. The word "ATOMAL" refers to information designated by the U. S. Government as "Restricted Data" or "Formerly Restricted Data" in accordance with the Atomic Energy Act of 1954, as amended. This information may be communicated by the Governments of the United States and the United Kingdom to NATO under the agreement between the parties to the North Atlantic Treaty Organization for cooperation regarding Atomic Information, June 18, 1964.

a. Classification of ATOMAL Information. ATOMAL information may be classified Top Secret, Secret, or Confidential. ATOMAL information is not classified RESTRICTED.

3. COSMIC. All NATO information that is Top Secret, whether ATOMAL or Non-ATOMAL, bears the additional designation "COSMIC" or is designated as "COSMIC TOP SECRET" information or "COSMIC TOP SECRET ATOMAL" information.

4. NATO RESTRICTED. Restricted is a security classification grading applied by NATO to information and material that requires security protection, but less than that required for Confidential.

0616. SECURITY OF CLASSIFIED NATO MATERIAL

1. COSMIC material will be handled, protected, and stowed as U. S. Top Secret material.

2. NATO Secret and Confidential material will be handled, protected, and stowed as are U. S. documents of comparable security classification, with one exception: NATO Confidential will be transmitted by U. S. Postal Service Registered Mail, regardless of its destination.

3. NATO RESTRICTED will be handled, protected, and stowed as U. S. Confidential material.

0617. STOWAGE OF NATO MATERIAL

1. NATO documents may be stowed in the same container with U. S. documents but shall not be mingled with U. S. documents. (Example: a file folder cannot contain both U. S. and NATO material. A file folder containing NATO material will be clearly marked with the NATO classification.)

2. NATO material is not to be retired to a U. S. Depository. When it is no longer needed, it should be destroyed. COSMIC documents will be destroyed through SPAWAR 00H.

0618. CLEARANCE

Prior to being authorized access to NATO classified information, personnel must be cleared for access to United States classified information of equivalent classification. All requests for access to NATO information will be submitted to the Security Office, in writing, and the request must be signed by a Division Head or higher. In SPAWAR, the Director, Security Office is authorized to grant NATO clearances up to and including COSMIC.

0619. HANDLING PROCEDURES WITHIN SPAWAR

1. Secret, Confidential and NATO-RESTRICTED material shall be processed and handled within SPAWAR by SPAWAR 18-512. Top Secret (COSMIC) material is controlled by SPAWAR 00H.

2. All NATO Secret documents directly received by SPAWAR personnel shall be delivered to SPAWAR 18-512 for control.

3. All incoming NATO Secret, Confidential and Restricted messages shall be delivered to SPAWAR 18-512 for processing and handling. Top Secret (COSMIC) is controlled by SPAWAR 00H.

4. Route sheets used to circulate NATO material within SPAWAR shall be conspicuously marked "NATO" by the records custodian. All classified NATO documents shall be logged in and out of each office receiving and releasing such documents.

0620. APPLICATION OF NATO CLASSIFICATION

SPAWAR does not have authority to apply COSMIC or NATO markings to any document it originates or receives, even though such documents are intended for entry into NATO. Appropriate markings are applied by the last U. S. agent on the NATO staff who actually introduces the document into NATO. U. S. information will be assigned and will retain an appropriate U. S. security classification. The foregoing does not preclude the use of the words COSMIC or NATO in the subject, heading or text of documents being prepared.

0621. U. S. DOCUMENTS TO BE ENTERED INTO NATO

1. Classified Documents. Except in cases where authority has been specifically delegated, documents intended for delivery into NATO shall be forwarded to the Security Office. The Security Office will evaluate foreign release aspects and refer to the NAVOTTSA for disclosure authorization.

2. Unclassified Documents. Documents containing unclassified information may be released into NATO by authority of the originators of the information. Such documents will be forwarded directly to the appropriate U. S. Documents Office for release.

20 DEC 1988

FOREIGN VISIT AUTHORIZATION

SERIAL NO.

DATE

NAVELEX 5512/6 (PART I) (Rev. 5-77)

TO: ELEX	ROOM	NAME(S) OF PERSON(S) TO BE VISITED

NAME OF VISITOR	SIGNATURE	RANK OR TITLE

NATIONALITY	AFFILIATION OF VISITOR	SPONSOR-AUTHORITY FOR VISIT

PURPOSE OF VISIT

DATE(S) AND TIME OF APPOINTMENT	SIGNATURE OF SECURITY OFFICER

20 DEC 1988

FOREIGN VISIT AUTHORIZATION

CONFIDENTIAL -

SERIAL NO.

DATE

NAVELEX 5512/6 (PART II) (Rev. 5-77)

TO: ELEX	ROOM	NAME(S) OF PERSON(S) TO BE VISITED

NAME OF VISITOR	SIGNATURE	RANK OR TITLE

NATIONALITY	AFFILIATION OF VISITOR	SPONSOR-AUTHORITY FOR VISIT

PURPOSE OF VISIT

DATE(S) AND TIME OF APPOINTMENT	SIGNATURE OF SECURITY OFFICER

TO BE COMPLETED BY ELEX 09G

1. DISCLOSURE LIMITATIONS:

TO BE COMPLETED BY PERSON VISITED AND RETURNED WITH PART I TO ELEX 09G BY NEXT WORK DAY

TO: ELEX 09G	INDICATE ACTUAL DATE OF VISIT	DURATION VISIT

2. PROVIDE BRIEF OUTLINE OF SPECIFIC SUBJECTS DISCUSSED AND CLASSIFICATION:

3. PROVIDE BRIEF OUTLINE OF ANY SIGNIFICANT INFORMATION LEARNED:

4. DID VISITOR EXPRESS INTEREST OR SPECIFICALLY REQUEST INFORMATION OUTSIDE THE SCOPE OF THE VISIT AUTHORIZATION? IF YES, PROVIDE EXPLANATION:

CONFIDENTIAL -	SIGNATURE OF PERSON VISITED	CODE & TELE NO.	DATE:

EXHIBIT 6-2

PROVIDED AS A SAMPLE ONLY

MEMORANDUM

From: _____
(Division Level or Higher)
To: SPAWAR Security Office (SPAWAR 10H)

Subj: REQUEST FOR APPROVAL TO VISIT LOCAL FOREIGN ENTITY

Ref: (a) (Current edition)

1. Pursuant to the requirements of reference (a), approval is requested for the following local foreign visit:

a. Name of person(s) making visit.

b. Purpose of visit in detail to include the advantages to the interest of the U. S. Navy and the classification of proposed U. S. disclosures.

c. Name and address of foreign entity.

d. Details causing the need for the visit, e.g., at the request of the foreign entity, to obtain information for SPAWAR program, etc.

_____
Signature (Divison level or higher)

DATE:

From: SPAWAR Security Office (SPAWAR 10H)
To:

1. Visit is _____ Approved _____ Disapproved

2. The following disclosure restrictions/special condition shall be observed:

3. The reverse side of this Memorandum shall be completed and returned to the Security Office no later than one working day from conclusion of visit.

EXHIBIT 6-2 (Cont'd)

EXAMPLE ONLY

DATE

From:
To: SPAWAR Security Office (SPAWAR 10H)

1. Names of person(s) visited.

2. Date of visit.

3. Brief outline of any significant information learned.

4. Indicate whether or not information was requested that was not authorized for disclosure, if yes, provide details.

_____
Signature (Person making visit)

CHAPTER VII

SECURITY AT SPAWARSYSCOM ACTIVITIES

0701. RESPONSIBILITY

1. Headquarters. The Director, Security Office, is responsible to the Commander, Space and Naval Warfare Systems Command for the provision of overall security direction to SPAWARSYSCOM activities and for monitoring of implementation and maintenance of adequate security procedures. In the execution of this responsibility, the Director, Security Office will:

a. Continuously review the level of security at all SPAWARSYSCOM activities and evaluate policy and performance effectiveness (to include the AIS security program.)

b. Direct through activity Commanding Officers/Commanders, specific actions which may be necessary to ensure a level of security consonant with existing regulations, laws and missions of the activities.

c. Conduct security training and seminars at Headquarters and activities.

d. Conduct on-site audits as frequently as deemed necessary in implementation of the foregoing responsibilities.

2. Activities. Commander/Commanding Officers, shall ensure implementation of the applicable requirements of this manual and those of reference (a) and OPNAVINST 5239.1A (series). Any special or unique security problem not covered by this manual or reference (a) shall be referred to the SPAWAR Security Office for resolution. Copies of all actions implementing the security program shall be furnished SPAWAR, attention Security Office.

CHAPTER VIII

OPERATIONS SECURITY

Section 1

POLICY AND ACTIONS

0801. GENERAL

DoD policy requires that each DoD component establish an Operations Security (OPSEC) program. OPNAVINST 3070.1A provides policy, guidance and direction for OPSEC matters within the Navy. CNO letter 5500 Ser 483C3/6S35506Z of 4 April 1986 provides criteria requiring OPSEC plans for protection of weapon systems test and performance data. This chapter implements Navy OPSEC policy, assigns actions and responsibilities for carrying out the Space and Naval Warfare Systems Command (SPAWAR) OPSEC program, and provides necessary direction and guidance to Headquarters Staff Offices, Program Directors, Program Managers, and field activities for OPSEC program accomplishment.

OPSEC REFERENCES

- National Security Decision Directive 298, National OPSEC Program, 22 January 1988.

- Department of Defense Directive 5205.2, DoD Operations Security Program, 7 July 1983.

- Joint Chiefs of Staff Publication 18, Operations Security, 15 December 1982, and OPSEC Survey Planning Guide (FOUO) 15 June 1983.

- OPNAVINST 3070.1A, Operations Security, 24 June 1985.

- CNO letter 5500 Ser 483C3/6S35506Z of 4 April 1986, OPSEC plans for protection of weapon systems test and performance data.

0802. SCOPE

This chapter is applicable to all personnel and operations of SPAWARSYSCOM, its activities and contractors.

0803. DEFINITION

Operations Security (OPSEC) is 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.

0804. CONCEPT

OPSEC is concerned with controlling detectable activities that would allow an adversary to prepare effectively for war, plan and conduct operations, and react to friendly operations. The total application of OPSEC extends from the tactical to the strategic level, from the present to the distant future, and in a variety of environments such as Headquarters offices, field activities, contractor facilities, laboratories and test ranges. OPSEC is a broad scope program concerned with the protection of information, classified or sensitive unclassified, which would be useful to an adversary. OPSEC serves to strengthen the traditional security programs. Moreover, OPSEC examines sensitive unclassified information and activities outside the normal scope of traditional security programs to identify information sources susceptible to hostile exploitation.

0805. POLICY

In accordance with OPNAVINST 3070.1A, OPSEC will be integrated with and used in every functional phase of staff operations, activity management, program contract accomplishment, research development, test and evaluation (RDT&E), procurement, and acquisition performed by SPAWARSYSCOM at all echelons of command. To this end, essential secrecy relating to military systems shall be preserved by the use of OPSEC principles and procedures to deny information of intelligence value to actual or potential adversaries, whenever possible.

0806. RESPONSIBILITIES

The Physical and Operations Security Division (SPAWAR 10H3) of the SPAWARSYSCOM Security Office (SPAWAR 10H) is the single point-of-contact responsible for all SPAWAR operations security matters. The Scientific and Technical Intelligence Office (00H) will provide intelligence support to assist in the OPSEC effort as requested. The Staff Offices and Program Directors/ Managers at Headquarters, SPAWARSYSCOM and the Commanders or Commanding Officers of all activities are responsible for activity OPSEC requirements.

0807. ACTION

1. Physical and Operations Security Division:

a. Update this operations security chapter providing OPSEC program guidance on an annual basis to complement specific security programs guidance provided elsewhere in this manual and other SPAWAR security directives.

b. Develop a SPAWARSYSCOM Command Operations Security Plan incorporating CNO guidance and Staff Offices, Program Director/Manager and field activity inputs.

c. Provide planning and analysis guidance, program assistance and oversight for Operations Security to SPAWARSYSCOM Staff Officers, Program Director/Managers and SPAWAR activities.

d. Chair the SPAWARSYSCOM Operations Security Committee, comprised of OPSEC coordinators and representatives of the traditional security disciplines, chartered to resolve OPSEC problems, establish policy and coordinate OPSEC planning and training actions.

e. Develop a comprehensive OPSEC training program.

f. Provide approval/disapproval of recommendations to CNO on all SPAWARSYSCOM requests for OPSEC waivers or exceptions.

2. SPAWARSYSCOM Headquarters Staff Offices/Program Directors/Managers:

a. Designate a senior technical staff member to be the OPSEC coordinator responsible for accomplishment of all OPSEC analysis, planning and OPSEC actions for their respective organizations.

b. Establish OPSEC requirements for each program/project and determine the classified and sensitive unclassified aspects of the program/project which must be protected.

c. Ensure, in coordination with SPAWAR 10H3, that the designated OPSEC coordinator and incumbents of OPSEC related positions/billets are briefed on their individual OPSEC responsibilities.

3. Commander/Commanding Officers of SPAWAR Activities:

a. Designate a senior member of the activity security staff as the activity Operations Security Officer and task that member with accomplishment of an activity Operations Security Program in accordance with this directive and its references.

b. Establish an Operations Security Committee chaired by the Operations Security Officer with a membership comprised of OPSEC coordinators.

c. Require each major element within the activity to designate a senior technical program staff member as an OPSEC coordinator responsible for accomplishment of all OPSEC analysis, planning and continuing OPSEC actions.

d. Identify positions/billets whose incumbents could be expected to have OPSEC analysis, planning, countermeasures, operating or other OPSEC responsibilities.

e. Develop and implement an OPSEC training program that includes technical OPSEC training for OPSEC coordinators and incumbents of positions with OPSEC responsibilities as well as awareness training for all personnel.

f. Provide the periodic OPSEC reports, required by reference (c), to SPAWARSYSCOM (SPAWAR 10H3) not less than 30 days prior to required OPNAV submission suspense dates.

g. Develop an activity Operations Security Plan that includes each activity mission/program/project/task that meets the criteria for inclusion in OPSEC planning. The OPSEC plan will be submitted to SPAWARSYSCOM (SPAWAR 10H) for approval before implementation.

h. Require an OPSEC plan or annex meeting SPAWARSYSCOM and CNO standards for all supported RDT&E, procurement or acquisition efforts involving classified or sensitive unclassified information.

i. Identify shortfalls in OPSEC requirements, include OPSEC in all program/budget reviews and take budgetary actions necessary to generate security projects on funding requests to correct shortfalls along with necessary waiver and exception requests needed on an interim or permanent basis.

4. All SPAWARSYSCOM Personnel:

a. Become familiar with and adhere to OPSEC practices and procedures applicable to daily operations.

b. Provide recommendations and suggestions for OPSEC related protection of classified or sensitive unclassified information to supervisors or the Physical and Operations Security Division, telephone (202) 692-8667 or Autovon 222-8651.

Section 2

OPERATIONS SECURITY PLANNING CRITERIA AND PROCEDURES

0808. OPERATIONS SECURITY PLANNING REQUIREMENTS

This section contains the OPSEC planning guidance and direction for SPAWARSYSCOM. SPAWAR activities will use their analysis of operations and programs as a precursor to development of OPSEC plans. Paragraphs 0811 through 0813 give the hostile threats, sensitive aspects/vulnerabilities and countermeasures information necessary to do an effective OPSEC analysis and develop an OPSEC plan. The formats for the various types of OPSEC plans are discussed in paragraph 0814.

0809. PLAN DEVELOPMENT CRITERIA

1. General OPSEC Planning Requirements. Any Headquarters Staff Office/ Program Director/Manager or activity Commanding Officer whose mission activities involve classified material or sensitive unclassified material, especially critical technology applications. Also, all RDT&E efforts must have an OPSEC plan if they involve classified information or sensitive unclassified information. Paragraph 0811.2. identifies activities, programs and operations, other than those in paragraph 0809.2. that must be provided OPSEC protection.

2. Protection of Weapon Systems Test and Performance Data. An OPSEC plan for the protection of Weapon Systems Test and Performance Data is required for each weapon system program and associated test and performance data. This plan may be the OPSEC plan for a staff code, Program Director or Manager responsible for a single weapon system program or project. There may be several weapon system OPSEC plans which must be integrated into an overall OPSEC plan for large multiple project programs at a field activity with diverse RDT&E or range operations. An OPSEC plan is required if any of the following criteria are met:

a. The research, exploratory development, or systems acquisition program includes technologies listed in the Military Critical Technologies List.

b. The program develops a weapon system, a weapon system component, or a method of operation in support of a weapon system. Examples include, but are not limited to:

(1) Sensors (passive or active).

(2) Data Processors.

(3) Fire Control Systems.

(4) Command and Control Systems.

(5) Weapon system hardware, e.g., missile launcher, gun mounts, etc.

(6) Ordnance.

(7) Test articles and related equipment.

c. Development, testing, or evaluation of a program generates classified or sensitive unclassified data or information. Examples include, but are not limited to:

(1) Accuracy. Precision with which the designated function (e.g., detection, range track, angle track) is performed.

(2) Miss Distance or CEP

(a) Miss Distance. Distance from a target within which the warhead is not effective.

(b) CEP. Radius of a circle around a target within which half of the weapons are expected to hit.

(3) Altitude Capabilities

(a) Maximum. Altitude beyond which performance is degraded to such an extent that failure is likely.

(b) Minimum. Altitude below which performance is degraded to such an extent that failure is likely.

(c) Optimum. Altitude spread at which performance is most satisfactory or effective.

(4) Counter-Measures Capability. Design features of a system which are intended specifically to overcome enemy interference. Electronic countermeasures are those measures which are used to defeat any enemy's use of electronic devices.

(5) Lethality. The ability to cause a specific degree of damage to a specific target.

(6) Maneuverability. Ability to change position or direction, a function of mass, velocity and design.

(7) Operational Readiness (Alert) Time/Time Cycle. Sequence and duration of important operations to be performed on or by the system or specified components of the system during a normal cycle or function (e.g., emplacement, loading and firing/launching, warm up prior to operation, etc.).

(8) Orbit/Trajectory. Path of travel of an object in space.

(9) Range

(a) Maximum. Greatest distance at which the system will perform satisfactorily.

(b) Minimum. Least distance from a target at which a system will perform as designed, usually a function of sensor capability.

(c) Optimum. Range and/or speed at which performance is most satisfactory or effective.

(10) Reliability. Probability that the designed function will be performed for a specified time and/or within specified limits.

(11) Resolution. Ability to analyze characteristics of a complex nature (e.g., signals, targets, signature characteristics, range, angle, etc.) and to distinguish between them.

(12) Numerical Frequency Bandwith. The upper and lower limits of that portion of the numerically designated band which is utilized in the system involved.

(13) Specific Frequency. Exact frequency within a numerical frequency band at which a system is designated to operate; or limited number of exact frequencies at which a system is designed to operate; or exact frequency set in at any one instance.

(14) Coding. Means by which a guidance system can discriminate between signals received.

(15) Sensitivity. Ability to receive signals.

(16) Speed/Velocity. Speed or velocity of the system during transit to perform its assigned mission.

(17) System Capacity. Maximum number of operations which the system can perform simultaneously in carrying out its designed function.

(18) Vulnerability to Countermeasures. Susceptibility to defeat by enemy actions usually based on information derived from laboratory tests or actual operational tests.

(19) Effectiveness Against Threats. Ability to perform assigned mission in the face of current or future foreign threats.

0810. OPSEC POSTURE ANALYSIS

Prior to issuance of an OPSEC plan and periodically thereafter, there is a requirement for each Program Director/Manager and major staff code in SPAWARSYSCOM Headquarters and SPAWAR activities to do an OPSEC analysis of

sensitive operations and projects (and those of contractors). This analysis is to determine how the threat and perceived vulnerabilities interact; requiring the institution of protective measures to eliminate or reduce vulnerability to acceptable levels. The completed analysis must be provided to SPAWARSYSCOM (SPAWAR 10H) by each major staff code and Program Director/Manager (or to the OPSEC Officer at each SPAWAR activity.) The OPSEC process involves five steps:

1. Identification of critical information.

2. Analysis of threats.

3. Analysis of vulnerabilities.

4. Assessment of risks.

5. Application of countermeasures.

It is important to remember that certain indicators and pieces of information may be pieced together to discern critical information.

0811. PLANNING GUIDANCE

1. The Hostile Threat. The Hostile Intelligence Threat to SPAWARSYSCOM and its field activities includes all three collection methods: Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Signal Intelligence (SIGINT). An initial summary of anticipated threat elements and probable collection methods is as follows:

a. HUMINT. Activities or situations that provide targeting information and human intelligence collection potential by a Hostile Intelligence Service are:

(1) Great quantities of unclassified, nonrestrictive correspondence, plans, reports, publications, technical data, etc., generated, utilized and discarded in the normal course of business.

(2) Open source materials, improperly disseminated sensitive information, voluntary public release, Freedom of Information Act (FOIA) releases, contractor releases, and releases accomplished through international agreements.

(3) Seminars and conferences attended by SPAWARSYSCOM personnel, industry representatives and others associated with SPAWARSYSCOM in some temporary or continuing manner.

(4) Presence of Foreign Diplomatic/Attache personnel, military exchange and liaison personnel, foreign visitors and foreign students visiting or residing in the or near SPAWARSYSCOM Headquarters and field activities.

(5) Aliens employed by suppliers, contractors, building owners and local civilian communities.

(6) Communist Bloc country crewman from ships docking at United States ports.

(7) Data facility and computer operations penetration by Hostile Intelligence agents and skilled computer hackers.

(8) Overt soliciations for information by individuals or organizations.

(9) Attempts to subvert employees.

b. IMINT. Imagery Intelligence threats are primarily directed at SPAWARSYSCOM field activities and may consist of the following:

(1) Photo satellite coverage of field activities and outdoor projects and project staging/storage areas as well as any operations or tests visible from above.

(2) Handheld photograph or covert television surveillance of documents, components, restricted areas or RDT&E facilities.

(3) Commercial and private aircraft photo coverage.

c. SIGINT. Signal Intelligence threats, including electronic intelligence, directed at SPAWARSYSCOM and its field activities are:

(1) Interception of microwave transmissions of AUTOVON and long distance telephone calls.

(2) Interception of telemetry, radar, automated information systems equipment, and other emissions by satellite, aircraft, afloat, or ground-based collectors.

(3) Interception of test facility voice communications.

(4) Electronic intercept/analysis of communications, intrusion detection systems, access control or voice circuits.

2. Sensitive Aspects of Operations. The following Essential Elements of Friendly Information (EEFI) whether they are facilities, information, or activities, present the initial range of potential targets for Hostile Intelligence collection. In most cases, the degree of sensitivity will vary from time to time depending on what is being processed, operated, tested, discussed or stored. Major code OPSEC coordinators will be responsible to the Physical and Operations Security Division of the Security Office (or the Operations Security Officer at field activities) for initial establishment of vulnerability and countermeasure requirements and subsequent mission-based adjustments to OPSEC requirements indicated in the final OPSEC plan for their office program or activity.

a. Classified Aspects. All classified information is exempt from release under exemption category 1 of the Freedom of Information Act (FOIA).

(1) SPAWARSYSCOM Staff Codes, Project/Program Directorates and SPAWAR Activities with Related Functions. Areas that involve classified weapons system technology, hardware, components, systems capabilities, and vulnerabilities. Classification guides outline the specific information and hardware directly associated with each weapon/electronic system.

(2) Command, Control and Emergency Operations. Procedures, information and activities.

(3) Communications Facilities. Includes the communications centers, crypto equipment, material, and vaults, SSO activities and communications panels, cabling, antennas, and wire closets.

(4) Special Projects. Of SPAWARSYSCOM, Navy and other agencies.

(5) Laboratory Facilities. Laboratory facilities, developmental information, software, hardware, and related activities in the areas of engineering, directed energy, simulation, sensors, propulsion control, and guidance and control.

(6) Testing. Test facilities, test results, equipment, ranges and testing activities may be classified or unclassified depending on the particular event/program being conducted. Included are any restricted areas in which test-related matters are conducted, discussed, analyzed or correspondence/materials stored.

(7) Arms/Ammunition/Explosive Storage Areas. The sensitivity and classification of information about these activities is based on what is being stored or the specific events involved. However, all are designated restricted areas or containers.

(8) Classified Material Storage Sites. The degree of sensitivity depends on classification of the stored materials.

(9) Automated Information Systems (AIS) and Networks to include associated remote and stand-alone or networked terminals that store or process classified information on or off-line.

(10) Intelligence Information and Activities. All

(11) Foreign Intelligence Information and Activities. All

(12) Future Weapon System Technology, Military Application Concepts and Developmental Designs. All, unless specifically exempted on a case-by-case basis.

(13) Data Exchange Agreements and Associated Information. All

(14) Threat Data. Intelligence threat data such as hostile intelligence targeting information and specific countermeasures to safeguard against a known threat.

(15) Planning Data. SPAWARSYSCOM Headquarters and SPAWAR Activity Emergency Action Plans, Crisis Management Plans, Communications Plans, Command and Control Plans, Operations/Exercise Plans, Naval Tactical Publications (NTP) for classified or critical technology equipments and security plans.

b. For Official Use Only (FOUO) Aspects. This sensitive category involves information for which public release may be denied under the Freedom Information Act (FOIA). Some areas of SPAWARSYSCOM information may meet the criteria for exemption. However, assignment of the FOUO protective marking requires that a case-by-case determination be made, based on review of exemption criteria in Navy directives pertaining to FOUO.

0812. VULNERABILITIES

The following general areas of vulnerability have been identified as requiring special precautions to avoid loss or disclosure of sensitive information.

1. Physical. Access to certain operational areas is based on possession of an authorized badge or visitor pass. Badges and passes are subject to forgery and detection of a good forgery is difficult. Any security system is subject to breakdown caused by carelessness, neglect or willful usurpation of controls by those responsible for protection. Controls are only as good as the personnel, whether they are contract personnel, civil service or military in the security force or employed/assigned to operating staff/activity codes.

2. Information. Poor housekeeping procedures or failure to follow handling instructions could lead to loss of documents or compromise by unauthorized personnel to include disaffected employees. Much sensitive information becomes available to the public and, therefore, to foreign collectors through open source documents. Most of it is in the form of bits and pieces released by SPAWARSYSCOM, other DoD agencies or contractors. Information is also available from the Defense Documentation Center, the Government Printing Office and the National Technical Information Center. Other operational documentation is widely distributed as unclassified material. Additionally, unclassified contracts can reveal technical descriptions, performance parameters and design data that must be considered as a vulnerable area. Some sensitive unclassified information never gets properly identified as such and therefore never gets placed under any kind of security control. This vulnerability is frequently revealed during OPSEC review for release of information which has been requested under the FOIA.

3. Personnel. Many personnel are OPSEC conscious in their daily routine; however, many have the philosophy that information is either classified or unclassified and if unclassified, no protection is required. Sensitive items, while not classified, present a vulnerable area. Various types of personnel support SPAWARSYSCOM on a daily basis. These include janitors, window washers, electricians, equipment repairmen, vendors, building maintenance personnel, etc. Some of these people may be cleared but none of them have a "need-to-know". With easy access they represent a threat to security. If these people are allowed to enter unattended into offices where classified documents are available, either on desks or in unlocked files, they could read, steal, copy or photograph sensitive information.

4. Technology Transfer. Research and development information may not receive adequate protection in the very early design and developmental stages or during the manufacturing process which may allow disclosure that could adversely affect subsequent military application. Sensitive technology is subject to unauthorized dissemination or possible transfer to hostile countries through improper public releases, technical seminars, Foreign Military Sales (FMS), request for information under the Freedom of Information Act (FOIA) and unauthorized releases on the part of contractors.

5. Communications. The geographical dispersal between SPAWARSYSCOM field activities, project offices, contractors and other DoD activities results in extensive use of long distance commercial and AUTOVON telephone systems. Telecopiers are also used in many areas. AUTOVON circuits are especially vulnerable in that they use microwave links which are vulnerable to intercept. Test activities involving telemetry, radar and voice communications are subject to monitoring by electronic intelligence gathering platforms, both in the air and on the surface. It must be assumed that all communications will be monitored.

6. Photography. SPAWARSYSCOM and its activities are vulnerable to photographic coverage by satellite, aircraft or handheld agent photography.

7. Reproduction Facilities. Reproduction facilities are readily available throughout SPAWARSYSCOM. While regulations pertaining to reproduction of classified defense information are adequate, reproduction facilities offer a fertile field for loss, compromise or theft of classified information. Copies can become jammed in the machines and left for uncleared personnel to find. Uncontrolled copies can become lost and be compromised without knowledge of the responsible official.

8. Conference Facilities. Meeting, conference and seminar sites are highly vulnerable since they are generally announced in advance. They are easily targeted and susceptible to unauthorized access, eavesdropping, improper disclosure to persons without "need-to-know" and inadequate protection of imparted information by attendees. Notes taken during sessions, handouts and subsequently provided transcripts or minutes are also potential problems.

9. Visitors and Foreign Liaison. There is often reluctance to challenge unbadged personnel. Failure to identify and control visitors is a serious violation of OPSEC principles. Also, foreign liaison personnel are assigned to certain operational areas under international agreement. All have limited accreditation. Although properly cleared they should not be privy to any and all information. Information provided beyond their "need-to-know" is a violation.

10. Computer/AIS. We are extremely dependent on automated information systems, computer resources and networks to store, retrieve, process and transmit vast quantities of products quickly and efficiently. Such systems are attractive targets to the hostile collector since physical or electronic access would represent a lucrative source for acquisition of a wide variety of operational information. Potential problems include equipment failure, procedural weakness or breakdown in security controls that may be caused by deliberate or inadvertent acts.

0813. COUNTERMEASURES

Countermeasures may reduce, eliminate, or minimize OPSEC vulnerabilities. The following countermeasures are general in nature and may be applicable to SPAWAR operations. Others are only applicable to either field or Headquarters elements. Each Headquarters or field activity must derive a practical mix of the type and degree of countermeasures to be used for their specific program, project or mission, based on their OPSEC analysis.

1. Security Education. The Security Education Program must provide knowledge and awareness. It must emphasize the threat from overt and clandestine hostile intelligence collectors in the areas of HUMINT, IMINT, and SIGINT. The entire work force must recognize their individual security responsibility. Managers and supervisors must provide leadership and require enforcement of regulatory controls to ensure a secure operating environment.

2. Coordination. Timely coordination between the Physical and Operations Security Division (SPAWAR 10H3) and functional elements in the Headquarters and at field activities on security matters will aid in early detection of problem areas and provide improved and expanded support to all activities. This will permit OPSEC principles, in general, to be given higher visibility and emphasis.

3. Guidance. OPSEC guidance and directives should be distributed throughout the Command Headquarters. These and other informational pamphlets, posters and announcements provide educational background and specific guidance for a variety of functional areas.

4. Program Review. An OPSEC committee must be established to guide, monitor and enforce OPSEC implementation. The committee will meet, as necessary, on the call of the chairman.

5. Access Control. Maintain strict control of identification badges and enforce the requirement to wear them. Prohibit duplicate badging and require owner certification in case of loss or theft. Do not indicate security clearance/access levels on badges.

6. Clean Desk Policy. Enforce the Command clean desk policy, particularly in highly sensitive areas.

7. Photographic and Recording Devices. Prohibit the introduction of personal cameras and recording equipment into sensitive areas.

8. Inspections and Surveys. Perform inspections and technical surveys of ADP facilities to determine areas of vulnerability and requirement for subsequent introduction of countermeasures.

9. Telephone Monitoring. Arrange for authorized telephone monitoring and use monitoring reports to improve telephone security. A security warning label should be affixed to unsecure telephones and personnel must be aware of availability and locations of secure lines.

10. Foreign Disclosures. Ensure all releases of information to foreign nationals are processed/cleared through the SPAWARSYSCOM Security Office (SPAWAR 10H).

11. Briefing of Foreign Nationals. Any briefings given to foreign nationals must be thoroughly sanitized in order to preclude unauthorized disclosure of information.

12. Foreign Liaison. Foreign liaison work spaces must be located to preclude unauthorized disclosure of information.

13. Visual Aids/Media/Displays. Ensure that chalkboards are protected from casual observation and cleared at the close of business. Charts, graphs, models, equipment parts, etc., must be given appropriate level of protection to prevent theft and/or unauthorized disclosure.

14. Visitor Control. Apply strict control over visitors. Designate and utilize visitor reception areas, visitor badges, registration and escorts, where required.

15. Conferences/Meetings and Briefings. Conference rooms and briefing areas must be sanitized prior to sensitive meetings and precautions exercised, during and after use.

16. Range/Test Area Security. Establish range/test area security prior to commencement of sensitive testing.

17. Communications Security. Voice radio communications should be kept to the minimum necessary to assure safety and continuity of operations.

18. Overhead Photography. Sensitive equipment and/or test range equipment should be obscured from overhead photography. Decoy devices should be considered.

19. Observation Points. Where possible and practical, observation points around and outside test ranges will be cleared to prevent agent photography.

20. Countermeasures Application. Any countermeasures utilized must be well conceived and practiced with caution. Redundant applications can do as much harm as good in certain scenarios. If deception methods are used it is important to forward proposed requirements to Chief of Naval Operations (CNO).

21. OPSEC Plan. Each program/project shall have a detailed OPSEC plan outlining specific Essential Elements of Friendly Information (EEFI) association with its activities and appropriate countermeasures necessary to protect the system. Identify those EFFI that are exempt from public release under the Freedom of Information Act (FOIA), and assign the For Official Use Only (FOUO) protective markings to material that meet the exemption criteria.

22. Sensitive Debris. Classification guides and project OPSEC plans should provide specific guidance on the recovery of sensitive hardware debris. This guidance, if appropriate, must be further outlined in the test plan provided to test facilities.

23. Countermeasures Requirements. Specify, in test plans, those protective countermeasures necessary to safeguard the component or system during testing. Test and evaluation facilities must refuse to test if this information is not furnished.

24. Communications Encryption. When possible and practical, telemetry and other test range communications will either be encrypted or utilize a hardwire system.

25. Retransmissions. Avoid the retransmission of telemetry and other test range communications over microwave links, via satellite or commercial land lines.

26. Power Regulation. When possible and practical, transmitter power will be regulated to provide a signal strength just sufficient to accomplish the job. This will help to prevent undesirable intercept of the signal at random locations on the periphery of test ranges.

27. Test/Threat Coordination. Coordinate testing and, where possible, provide "real-time" threat data to permit test shutdown when collection platforms are present in the area. The threat situation must be checked prior to commencement of test activities. Provide test facilities information about any specific hostile collection activities directed against the particular project/program.

28. Technical Data Distribution. Limit distribution of technical data packages to those agencies/offices that have an absolute "need-to-know."

29. Facility Parking. Prohibit parking of large non-Government vans or motor homes within 500 feet of building containing AIS facilities or other sensitive electronic processing equipment, if possible.

30. Filtering Devices. Utilize filtering devices on AIS and word processing equipment to preclude intercept of compromising or unintentional intelligence bearing signals.

31. Public Release Review File. Establish, within each program/project office, a central point for release of information to the public. Maintain a historical file of released information so that each proposed public release can be compared against previous releases. The purpose of such comparison is to help avoid eventual total release through piecemeal methods.

32. Publications Screening. Information about SPAWARSYSCOM managed systems for possible release into the public domain must receive a security review prior to exposure to resources for publication. Contractors must be required to clear all proposed releases through the project office.

33. RD&TE Facility Access. Deny use of all RDT&E activities, facilities and ranges to persons not authorized entrance.

34. Emanations Reduction. Require removal of extraneous wiring from sensitive areas simultaneously with remodeling contracts.

0814. OPSEC PLAN FORMAT AND PREPARATION

Exhibit 8-1 contains the OPSEC Plan format that will be used by all SPAWARSYSCOM Program Directors/Managers, staff offices and SPAWAR activities for preparation of OPSEC plans. Exhibit 8-2 will be used for the development of an OPSEC Plan for protection of weapon systems test and performance data.

EXHIBIT 8-1

COMMAND/STAFF OPSEC PLAN

References:

1. Purpose. To establish an Operations Security Plan for (name). The mission of (Command, organization, staff office, etc.) is:

2. Scope. The provisions of this plan apply to Command/staff elements assigned functions related to the following operations and other activities:

a. Those initiated, planned, or conducted by the Command/staff (specify by type).

b. Those supported by the command/staff (specify by type).

3. Structure

a. The organizational element responsible for OPSEC is (name).

b. Other specific organization(s) to address OPSEC (if any).

c. OPSEC responsibilities of other Command/staff elements are (state Command/staff element and specific OPSEC-related responsibilities (planning, training, etc.).

4. Training

a. Orientation. Describe a program to provide OPSEC orientation for Command personnel when they report to or are hired by the Command/staff.

b. Continuing Awareness. State how a Command OPSEC awareness program will be conducted. Such a program could consist of posters, plan of the day, notes, discussions of specific problems, routing of case studies or lessons learned, etc.

c. Planning Skills. Outline a training program to provide training in OPSEC planning to incumbents of billets whose functions require OPSEC planning skills. Billets should be listed in Appendix A of this plan.

5. OPSEC Planning Guidance. Include data to support OPSEC planning in accordance with command/staff needs.

VI. Alternate Methods to provide Countermeasures. Where existing capabilities (described in Section V) are insufficient to meet requirements (described in Section IV), describe, in detailed narrative form, alternate methods of providing protection to data.

VII. Additional Capabilities required to provide Countermeasure: It is the activity Commander's responsibility to identify shortfalls in the capability to provide countermeasures necessary to protect weapon systems data to the appropriate remedial authority. Where the aggregate of capabilities (Section V) and work-arounds (Section VI) are insufficient to meet requirements (Section IV), the shortfalls should be described in specific details and forwarded to SPAWARSYSCOM (SPAWAR 10H).

a. State requirements for secrecy about Command intentions, capabilities, operations, and other activities.

b. State OPSEC plans required prior to, during, and after operations and other activities initiated, conducted, or supported by the Command, including requirement to be met by other Commands/staff prior to the provision of support to them.

6. OPSEC Posture Evaluation

a. Outline a program to periodically survey (informal or formal) the Command OPSEC posture.

b. State requirements and procedures to monitor and evaluate the effectiveness of OPSEC measures intended to preserve essential secrecy for operations and other activities.

EXHIBIT 8-2

FORMAT FOR PLANS TO PROTECT WEAPON SYSTEMS TEST AND PERFORMANCE DATA FOR NAVY LABORATORIES

I. Activity Description

II. Data requiring protection

III. Threat, vulnerabilities, and countermeasures

IV. Required capabilities to provide countermeasures

V. Existing capabilities to provide countermeasures

VI. Alternative measures for protection of data

VII. Additional capabilities required to protect data

NOTE: A plan for the protection of weapon systems test and performance data is required for each activity under SPAWARSYSCOM cognizance that deals with weapon systems projects. At each laboratory this plan will normally constitute a subset of the overall activity OPSEC plan and must address each weapon system that the activity's mission involves.

EXHIBIT 8-2 (Cont'd)

DIRECTIONS FOR PLAN DEVELOPMENT

I. Activity Description. Briefly describe the activity's mission. The description should emphasize the current aspects of research, development, testing, and evaluation (RDT&E) support capability.

II. Data Requiring Protection. Describe the data that the activity will generate which will require protection. Reference (c) provides a listing of those types of data which require protection.

III. Threat, Vulnerabilities and Countermeasures. Use the maxtrix found on page 8-D-1 to provide a summary of threat, vulnerabilities and countermeaures associated with the activity. Threat, in the context of this plan, is defined as the intent and capability by adversaries to acquire information/data about Navy assets, their intended use and their performance parameters. Assistance in determining threat can be obtained from the SPAWAR OPSEC officer and local Naval Investigative Service Agent.

Vulnerabilities are defined as any activity mission support function which allows a hostile intelligence collection effort to gain critical and sensitive information/data, classified or unclassified. Countermeasures are defined as technical, procedural or administrative means to deny access to or acquisition of critical and sensitive information/data concerning weapon system development.

IV. Required Capabilities to Provide Countermeasures. In detailed narrative form describe specifically the activity capabilities to provide countermeasures necessary to protect the data described in Section II against the threat summarized in Section III.

V. Existing Capabilities to provide Countermeasures. In detailed narrative form describe specifically which of those capabilities described in Section IV currently exist or will exist at the time they will be required by tasking authority. Required capability must be defined as to availability by FY/Qtr. The description should include those capabilities necessary to control/protect data associated with the RDT&E of weapon systems.

APPENDIX to EXHIBIT 8-2

e. A/V, T = Asset/vulnerability and threat with no countermeasure in place or available by date of need.

Configurations (a) through (d) constitute a statement that all issues and inputs have been considered and attended to and that the protection of weapons system test and performance data will be accomplished in the best practicable manner possible.

Configuration (b) constitutes a statement that assets/vulnerabilities, and threats against them, exist for which there is no suitable countermeasure available. A determination of Configuration (e) will generate three (3) subsequent actions:

(1) Examination and use of approvable work-arounds.

(2) A determination to continue, or not, R&D or T&E efforts in the current environment.

(3) Ensurance that perceived countermeasure deficiencies are resolved either by correction within existing resources or by documenting deficiencies and forwarding them to the appropriate superior Command.

5. Matrix Notes. The following notations are general aids to properly completing the Matrix:

a. Definitions/descriptions of threat, vulnerability and countermeasures are to be found in OPNAVINST 3070.1A and other Navy Instructions, guidance and references.

b. Matrix is suggestive, not comprehensive; additions to any of the three dimensions are dependent on the specifics of individual weapons systems, RDT&E activities, technologies involved, etc.

c. Responsibility for different elements of asset/vulnerability and countermeasures are shared by various Commands, funding, sources, and functional areas (i.e., airborne encryptors = program sponsor, ADP systems = facilities, physical security controlling guidance = OP-09N, etc.).

d. Allow appropriate lead time for Matrix construction sufficient to identify and correct problem areas by date of need.

EXHIBIT 8-2 (Cont'd)

PROTECTION OF WEAPON SYSTEMS TEST AND PERFORMANCE DATA PLAN

APPROVAL FORM

This form is to certify that the plan has been reviewed and approved for:

_____
(Activity Name)

APPROVED:

(Operations Security Officer) _____ _____
(Name and Title) (Date)

(Activity Command) _____ _____ ____ ____
(Name and Title) (Date) YES NO

Commander, Space and Naval Warfare Systems Command

Approved _____ _____
(Signature) (Date)

APPENDIX 1 TO EXHIBIT 8-2

NAVY LABORATORY PROTECTION CAPABILITY MATRIX

1. General Methodology: Navy laboratories should employ all existing resources that can materially aid in the preparation of individual activity protection plans. At a minimum, the following assets should be utilized:

a. Program/Project Managers and associated personnel conversant with technical aspects of weapon systems.

b. Intelligence support (threat) - NIS/STILO.

c. Technical security support (vulnerabilities/countermeasures) - COMNAVSECGRU.

d. Command Security Manager.

e. Applicable support functions.

2. Matrix Inputs: The Navy laboratory protection capability Matrix is designed as a three dimensional presentation of the shore activity environment in which the RDT&E of weapon systems will occur. When filled out, the Matrix is to be used as a control document and decision making tool in determining the level of security available to any program at any point in its development.

Prior to completing the Matrix, those responsibile for its preparation should conclude the following actions:

a. Define the Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Imagery Intelligence (IMINT) threats to the Command.

b. Answer the questions, "What are the vulnerabilities associated with this Command's assets/capabilities?", "What information, if compromised, would lead an adversary to the design of countermeasures to the weapons systems under development?"

c. Determine the data generating/handling requirements associated with the Command (i.e., telemetry, radar emissions, AIS networks, technical reports, etc.).

d. Establish the activity's capability to control/safeguard critical/sensitive data (countermeasures.)

APPENDIX I to EXHIBIT 8-2

3. Completing the Matrix. Using the Matrix key, fill out the Matrix as follows:

A/V - Asset/Vulnerability. Those support elements necessary to the RDT&E of a weapons system (i.e., receiving a telemetry stream, processing data on an ADP system, transmitting data to a contractor's facility, discussing program information via telephone, publishing interim results, etc.). The word "asset" indicates both data generators and directed Navy security assets. The word "vulnerability" indicates data collection potential or system deficiency from a security perspective.

T = Threat. The intent and/or capability to collect information of intelligence value. Threat is the combination of targeting, collection platform and opportunity.

C = Countermeasure. Procedural, administrative and/or technical interdictions between the hostile threat and the friendly vulnerability.

A/V will be placed in the appropriate box of the Matrix if the activity requires/possesses any of the enumerated assets. The A/V will also be used if any of the assets are judged to be deficient (vulnerable) from the point of view of being able to protect adequately the data associated with weapons system development.

T will be placed in the appropriate box of the Matrix if there are discernable threats (platforms), actual or potential, against the activity or any of its constituent parts. Threat should be considered as it relates to the technology, key personnel, individual program or data types listed in reference (c).

C will be placed in the appropriate box of the Matrix if the activity requires a countermeasure to a specific threat and/or vulnerability.

4. Use of the Matrix. Upon completion, each of the Matrix boxes will have one of five possible configurations.

a. Empty or N/A = No asset/vulnerability, no threat, no countermeasure.

b. A/V only = Asset/vulnerability but no discernable threat, hence no necessary countermeasure.

c. T only = Threat but no asset/vulnerability, hence no countermeasure.

d. A/V, T, C = Asset/vulnerability and threat indicates a mandatory employment of countermeasure(s), and the countermeasure is available.

ASSET/ VULNERABILITY	THREAT										COUNTERMEASURES
	HUMINT	IMINT	ACINT	VISINT	PHOTINT	ELINT	COMINT	FISINT	EMINT	GENINT	
Telemetry											Encryption, power reduction, deception, workarounds
Telephone											Encryption, awareness
Facsimile											Encryption
Communications											Encryption, protected distribution systems
Emissions											Low power, deception, jamming, shielding
Automatic Data Processing											OPNAVINST 5239.1A, certification of systems, passwords, software control
Video											Encryption, physical safeguards, classification mgt
Physical Security											OPNAVINST 5530.14A, IDS, guards lighting, fencing, access control
Information Security											OPNAVINST 5510.1G, OPNAVINST 5510.161
Personnel Security											OPNAVINST 5510.1G, BIs, awareness, clearances, need-to-know, training
Open Source Literature											OPNAVINST 5510.161, awareness of review for public release, distribution statements, general awareness
Indicators											*Cover/deception, information control
Observables											Cover and deception
Contractors											Use of DD254 & DD1664 to specify protection requirements, DIS, FAR Part 35. Sub-Chapter F
Work Spaces											TEMPEST, safes, TSCM, awareness

ACTIVITY PROTECTION CAPABILITY MATRIX

*NOTE:
Cover and deception operations require CNO approval prior to initiation of any effort.

KEY: A/V = Asset/Vulnerability
T = Threat
C = Countermeasure

CHAPTER IX

AUTOMATED INFORMATION SYSTEM SECURITY

SECTION 1

0901. GENERAL

1. This chapter sets forth those policies, requirements and guidelines necessary for consistent and effective implementation of the Automated Information System (AIS) security program throughout the Space and Naval Warfare Systems Command (SPAWARSYSCOM).

2. The SPAWAR AIS security program involves the application of the basic policy and principles of security as they relate to AIS which handle classified, sensitive unclassified and unclassified information where the use of computer technology introduces vulnerabilities uniquely attributable to that technology. This chapter also defines policy requirements to implement Office of Management and Budget (OMB) circular A-130, DoD Directive 5200.28 and related SECNAV and OPNAV AIS security directives.

0902. SCOPE

This chapter applies to all SPAWAR activities to include:

1. SPAWAR HQ organizational components

2. SPAWAR activities

3. SPAWAR sponsored contractors who operate contractor owned or SPAWAR owned/controlled AISs, networks or computer resources on or off SPAWAR premises.

4. All AISs, networks and computer resources designed, developed or procured by SPAWAR HQ components and SPAWAR activities.

5. Joint service or other AISs, networks or computer resources operated but not owned by SPAWAR, when security requirements have not been specified.

6. Printing and imaging equipment or systems which are part of an AIS, connected to a network or driven by process control or embedded computers.

7. Classified, sensitive unclassified and unclassified information.

0903. DEFINITIONS

The following factors are essential for compliance with the DON and SPAWAR AIS security program concepts. Additional factors and their definitions are found in Section 3.

1. Accreditation. The formal management authorization for operation of a specific application of an AIS, network or computer resource, based on the results of a security certification and risk assessment. It is a formal decision by the Designated Approving Authority (DAA) that a system is approved to operate in a particular security environment meeting a prescribed set of security requirements.

2. Certification. The formal statement made in support of the accreditation process, which establishes the extent that a specific application of an AIS, network or computer resource meets a set of specified technical security requirements.

3. Designated Approving Authority (DAA). The official who has the authority to decide that an AIS, network or computer resource may operate based on an acceptable level of risk considering the operational need for, and threats to, the system; and who is responsible for issuing an accreditation statement that records the decision.

0904. CONCEPTS AND OBJECTIVES

To ensure the availability of reliable information and automated support required to meet the DON and SPAWAR mission by adequately protecting all automated information systems, networks and computer resources against accidental or intentional destruction, unauthorized disclosure, denial of service and unauthorized modification. This objective will be met by ensuring that countermeasures provided by physical, administrative and operational procedures, personnel, communications, emanations, hardware, software and data security elements are collectively adequate to protect against such events as material hazards, fire, misuse, espionage, sabotage or malicious acts.

0905. GENERAL POLICY

1. It is the policy of the Commander, Space and Naval Warfare Systems Command that all AIS, networks and computer resources operated or developed by SPAWARHQ components and SPAWAR activities meet current and additional DoD, SECNAV, OPNAV and SPAWAR security policy requirements for those systems, networks and computer resources. Included within this policy are the minimum program re- quirements in Section 2 of this chapter, additional requirements issued by higher level DAAs.

2. SPAWAR AIS and networks which process classified data may do so only if accredited or granted interim approval to operate (IATO) by the appropriate DAAs or office of primary responsibility.

3. Managers within SPAWAR place emphasis on and ensure that security requirements are implemented for AIS, networks and computer resources which are under their operational, developmental or acquisition control.

4. The use or introduction of AIS software acquired from private (non-government or non-contracted) or public domain sources is prohibited within SPAWAR unless approved by the Automatic Data Processing Security Officer (ADPSO) who has security responsibility for the cognizant system.

5. The use of SPAWAR AIS, networks and computer resources is restricted to official business purposes only.

6. The introduction and use of privately owned AIS devices to process official data/information within SPAWAR is prohibited unless approved by the activity ADPSO.

7. The reproduction and application of copyrighted software within SPAWAR must be accomplished under existing legal requirements. Questions regarding this policy should be referred to SPAWAR 00C via SPAWAR 10H2.

8. Emanations (TEMPEST) requirements of OPNAVINST C5510.93 (series) are met for SPAWAR operated or controlled AIS, networks and computer resources.

0906. RESPONSIBILITIES AND AUTHORITY

To ensure the requirements of the DoD, Navy and SPAWAR AIS security programs are developed, implemented and maintained, responsibilities and authority are assigned as indicated:

1. <u>SPAWAR Headquarters</u>

a. The Director of Security (SPAWAR 10H) is designated as the primary agent for the management, execution and oversight of the SPAWAR AIS security program for operational AIS, networks and computer resources.

b. SPAWAR 10H is authorized to act as the SPAWAR DAA and is authorized to grant or endorse request for security accreditation or interim approval to operate for AIS and networks operated at SPAWAR Headquarters and SPAWAR activities. This includes request which must be forwarded to higher level DAAs.

c. Deputy/Deputy Assistant Commanders, Program Directors, Project Managers and Heads of Staff Offices within SPAWARHQ are responsible for ensuring that the fundamental AIS security concepts of this Chapter, and other applicable security directives are applied to AIS, networks and computer resources which are under the management of their organizational components. Included within this responsibility are:

(1) The identification and appointment in writing of an individual to be the automatic data processing security officer (ADPSO) to act as the focal point for AIS security matters within their component.

(2) Ensure that the AIS security policies of paragraphs 0905, 0907 and Section 2 of this Chapter and higher level authority AIS security policies are executed for AIS, networks and computer resources under their operational, developmental and acquisition control.

(3) Ensure that Information System (IS) Project Managers for mission support (non-tactical) AIS forward Mission Element Needs Statement (MENS), System Decision Papers (SDPs) and/or Abbreviated System Decision Paper (ASDP) to SPAWAR 10H2 for AIS security review prior to submission to the SPAWAR IS management division (SPAWAR 18-4).

d. The SPAWAR Automatic Data Processing Security Manager (ADPSM), (SPAWAR 10H2) is the SPAWARHQ ADPSO and is the appointed single focal point for SPAWAR operational AIS security program implementation matters and is assigned the following responsibilities:

(1) General management, administration, coordination, implementation and monitoring of the SPAWAR AIS security program, including security analysis, risk management, security test and evaluation (ST&E), inspection and security accreditation.

(2) Ensuring that the policies and requirements of DoD, Navy and SPAWAR AIS security instructions are implemented and that security operating procedures are prepared, issued, and maintained for SPAWAR operated systems and networks in accordance with applicable security, life cycle management, communications, emanations, contingency planning and other security directives.

(3) Ensuring that the minimum AIS program requirements of Section 2 and additional policy of higher level DAAs are implemented within SPAWAR.

(4) Monitoring implementation of such directives and procedures and directing actions appropriate to remedy security deficiencies and/or to enhance the AIS security posture of SPAWAR.

(5) Take action to ensure ADPSOs, network security officers (NSOs) or other AIS security officials are identified and appointed for SPAWARHQ components, SPAWAR activities, AIS, networks, and computer resources.

(6) Ensuring that AIS and network security activities, policies, requirements, and directives, as related to SPAWAR, are enforced and that conflicts of interest, responsibilities, and functions are resolved. The SPAWAR ADPSM is authorized:

(a) To communicate directly with applicable SPAWAR DAAs and other SPAWAR management elements regarding the application of the SPAWAR AIS security program and related matters of substance.

(b) To request SPAWARHQ components and SPAWAR activities to provide support as required for the accomplishment of the SPAWAR AIS security program objectives.

2. SPAWAR Activities. Commanding Officers and Commanders of SPAWAR activities are responsible for ensuring that:

a. AIS, networks and computer resources operated, developed or acquired under their command receive the appropriate security certifications or accreditations.

b. Act as the designated approving authority for AIS, networks and computer resources under their jurisdication. In those cases where DAAs are restricted to higher level authority the request for security accreditation will be forwarded to the appropriate DAA via SPAWAR 10H for mission support AIS, networks and computer resources. Accreditation support documentation specified by the DAAs will be forwarded with the request(s).

c. Identify and appoint in writing an individual to be the activity's ADPSO for AIS security program matters. The activity's ADPSO should have direct access to the Commanding Officer and/or the Commander of the activity. The activity ADPSO will ensure that:

(1) The AIS security and minimum requirements of this Chapter and higher level policy requirements are executed for AIS, networks and computer resources at their activity.

(2) Applicable number(s) of automatic data processing system security officers (ADPSSOs), NSOs, and other AIS security officials are identified, appointed and trained.

(3) AIS security requirements are identified and specified in acquisition and procurement documentation for mission support AIS acquired under SECNAVINST 5231.1 (series) and SPAWARINST 5231.1 (series).

(4) An activity accreditation schedule (AAS) is developed, maintained and executed for operational and planned AIS, networks and computer resources under their cognizance. The AAS will identify AIS, document accreditation elements and establish plan of action and milestone (POA&M) dates for completion of the accreditation process.

(5) Questions on policy issues in regard to SPAWAR or higher level AIS security program matters be directed to the SPAWAR ADPSM, SPAWAR 10H2.

0907. SPECIFIC POLICY

1. In addition to the general AIS security policy provided in paragraph 0905 all SPAWAR AISs, networks and computer resources will be protected by the continous employment of appropriate protective measures. The following policies apply:

a. Accreditation. AISs, networks and computer resources will be accreditated by the appropriate DAA based on a certification and risk management process.

(1) AISs not accredited may operate if the appropriate DAA has issued an Interim Authority To Operate (IATO) for a period not to exceed one year.

(2) An accreditation or IATO may be issued for an entire system or group of systems in those instances where the DAA has determined that such a "blanket" IATO or accreditation represents the most efficient means of maintaining system operability while ensuring security.

(3) Accreditations will be reviewed at least once every three years and when changes to the functionality, architecture, data processed, user population or environment result in a change to the exposure to harm of the AIS, network or computer resource. If no such change has taken place, the accreditation may be reissued based upon a thorough review of the previous accreditation documentation.

(4) Accreditation of embedded computer systems remains the responsibility of their DAAs.

(a) Program sponsors will require that program managers certify that systems satisfy security requirements, and that end users are provided with standard operating procedures and documentation to permit accreditation with minimal effort.

(b) DAAs may elect to group-accredit specific systems under their operational control in order to relieve subordinates and end users of this administrative burden. With the concurrence of the OPRs, DAAs may issue an accreditation covering the entire population of a given system.

b. Life Cycle Management (LCM). Action shall be taken throughout the life cycle of SPAWAR AIS, network or other computer resource to ensure compliance with security policies.

(1) SPAWAR HQ components and activities are responsible for ensuring the early and continuous involvement of the users, security staff, data owners, DAAs, and OPRs in defining and implementing security requirements of the system.

(2) Statements of security requirements are mandatory in the acquisition and procurement specifications for all SPAWAR AISs, networks or other computer resource.

(3) To the maximum extent possible, security will be built into systems such that system users are relieved of the details of assessing, testing and developing security for that system.

c. Risk Management. DAAs will ensure that a continuing risk management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets or denial of service. Risk management shall be applied throughout the life cycle.

d. Contingency Planning. Contingency plans shall be developed and, to the maximum extent feasible, tested to ensure that they function in a reliable manner and that adequate backup functions are in place to ensure that critical service is maintained.

(1) DAAs are responsible for determining contingency plan requirements for systems under their purview.

(2) Plans shall be tested prior to accreditation or re-accreditation under realistic operational conditions to the maximum extent feasible.

(3) If contingency plans cannot be tested realistically prior to accreditation, the DAA may issue an IATO pending testing within one year.

e. Designated Approval Authority. The DAA is responsible for formally granting authority to operate systems based upon an acceptable level of risk.

(1) DAA responsiblity is vested in Commanding Officers or Commanders unless otherwise specified by higher level authority.

(2) The senior DON official utilizing a Joint Service or non-DON AIS, network or computer resource shall be the DAA for the DON. In the case of cryptologic systems and networks supporting cryptologic functions or Sensitive Compartmented Information (SCI)/intelligence systems, the DAA shall be established by higher level authority.

(3) A single overall DAA will be designated and responsibilities established by Memorandum of Agreement or Understanding where there are networks which include systems or sub-networks having different DAAs except in the case of cryptologic or SCI systems. Paragraph 5.b. applies.

f. User Access. An AIS, network or other computer resource will function in accordance with the "least privilege" principle (as defined in DoD 5200.28-STD "Orange Book") so that each user is granted access only to the information to which the user is entitled by virtue of their security clearance or formal access approval and only the resources necessary to perform assigned functions. In the absence of a specific positive grant of access, user access defaults to no access.

g. Security Implementation. When specified by DOD, SECNAV or OPNAV all computer resources that process or handle classified or sensitive unclassified information shall implement Class C2 functionality (Controlled Access Protection) as defined in DoD 5200.28-STD.

(1) Class C2 protection provides for discretionary access control, memory clearing before reuse, individual accountability and audit trails. Implementation of Class C2 security for all appropriate systems by established time frames may not be feasible if the required software technology is not available. Higher level authorities may specify exceptions to this policy.

(2) Personal computers will be protected by hardware, software and security operating procedures to provide reasonable security until such time as effective C2 Class protection becomes available for personal computers.

h. AIS Security Program Elements. SPAWAR DAAs, responsible AIS security officials, managers of SPAWAR AIS, networks and computer resources and program and project managers must place special emphasis on the following elements:

(1) AIS Security Training and Awareness: All hands, civilian and military, shall receive appropriate training and awareness information, commensurate with their duties and responsibilities.

(2) Access Control: Physical, procedural and technical controls must be put in place to ensure that only authorized personnel with need-to-know are allowed to manipulate data. In the absence of positive grants of access, systems should default to no access (least privilege).

(3) Audit: Systems must be developed to have appropriate audit features, both financial and security, built-in and protected from tampering throughout their life cycles.

(4) Vulnerability Reporting: Vulnerabilities of existing systems must be identified and fixes developed to prevent exploitation. Vulnerability reporting will be accomplished under DOD INST 5215.2 or under Navy reporting requirements.

(5) Risk Assessment: Appropriate quantitative and qualitative methods of risk assessment shall be developed and promulgated to provide decision makers with management tools to aid in securing systems without undue administrative burden; automation of risk assessment shall be used to reduce the burden wherever feasible.

(6) Security Test and Evaluation (ST&E): Systems shall be subjected to a site and system specific ST&E to ensure that the environmental and operational security requirements have been met. When feasible, ST&E shall be conducted by a third party approved by the DAA.

(7) Contingency Planning: Contingency plans are necessary for all systems essential to performance of an activity's operational mission. A contingency plan is not complete until it has been tested under realistic operational conditions. The complexity of the contingency plan is dependent upon the complexity of the system and its need for mission performance.

(8) Communications Security: Protective measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications. Managed by CNO (OP-094) under CSP-1, Communications Security Policy Manual.

(9) Personnel Security: Procedures for screening all individuals to ensure a level of trustworthiness which is commensurate with the duties of the individual. Managed by CNO (OP-09N) under OPNAVINST 5510.1 (series), Department of the Navy information and Personnel Security Program Regulation.

(10) Physical Security: Physical measures designed to safeguard personnel, prevent unauthorized access to equipment, installations, material, computer media and documents, and to safeguard against espionage, sabotage, damage and theft. Managed by CNO (OP-09N) under OPNAVINST 5530.14, Naval Physical Security and Loss Prevention Manual.

(11) Emanations Security (TEMPEST): TEMPEST is the study and control of spurious signals emitted by electrical equipment. Managed by CNO (OP-09N) under OPNAVINST C5510.93, Navy Implementation of National Policy on Control of Compromising Emanations (U).

SECTION 2

SPAWAR AIS SECURITY

0908. MINIMUM PROGRAM REQUIREMENTS

SPAWARHQ components and SPAWAR activities will take such action as necessary to ensure that these minimum requirements are satisfied in a cost effective manner to meet the unique needs of their AIS, networks and computer resources. Higher level DAAs and Navy OPRs may issue more stringent requirements in additon to these.

1. Individual Accountability. Access to SPAWAR AISs, networks and other computer resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

2. Physical Control. AIS, networks and other computer resources will be physically protected against damage and unauthorized access.

3. Data Integrity. Each data base collection of data elements in an AIS will have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement and disposition will be governed on the basis of classification, sensitivity, type of data, need-to-know and other restrictions.

4. Marking. Permanent human-readable output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (i.e., the AIS has the capability to produce the markings) or may be done manually. Automated markings on output will at the highest level of data processed by the system unless the security features and assurances of the AIS meet, at a minimum, the requirements of a Class BI trusted computing base in DoD-STD-5200.28-STD.

5. Access. There shall be in place an access control policy for each AIS. It shall include features and/or procedures to enforce the access control policy of the information contained within the AIS. The identity of each user authorized access to the AIS shall be positively established prior to authorizing access.

6. Network/Communication Links. All communications circuits will be secured in accordance with the communications security program. Those handling plain text classified will be installed in an approved protected distribution system (PDS). For purposes of accreditation, a network shall be treated as either an interconnection of AISs (which may, themselves, be networks) or as a single distributed system.

7. Accreditation. Each AIS, network or computer resource shall be accredited to operate in accordance with a DAA-approved set of security requirements.

8. Risk Management. There shall be in place a risk management program to determine how much protection is required, how much exists and the most economical way of providing needed protection. Risk assessments shall be conducted:

a. Prior to design approval.

b. To support accreditation.

c. Whenever there is a significant change to the system.

d. At least once every three years.

9. Certification. Project or program managers shall certify to the users and the DAA that the systems security requirements have been satisfied and specify any constraints on the system or its environment necessary to maintain the certification.

10. Contingency Planning. SPAWAR HQ components and SPAWAR activities will develop and test a contingency plan, addressing both automated and manual backup systems, to provide for the continuation of its mission during abnormal

operating conditions. The contingency plan will be developed, tested and maintained to ensure continued performance of mission support and mission critical functions. It must be consistent with disaster recovery and continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems.

11. Internal Security Mechanisms. After the system becomes operational, software and files providing internal security controls, passwords or audit trails will be safeguarded at the highest level of data contained in the AIS, network or computer resource. Access to internal security mechanisms will be controlled on a strict need-to-know basis.

12. Encryption. Encryption methods, standards and devices used to protect classified data processed by an AIS, network or computer resource must be National Security Agency approved.

13. Emanations Security. AISs, networks and computer resources shall comply with the emanations security (TEMPEST) requirements of OPNAVINST 5510.93E.

14. Privately Owned Resources. Use of privately owned or leased personal computers, microcomputers or Public Data Networks to conduct official SPAWAR business in a SPAWAR workplace or connected to a network is allowed only with the prior written authorization of the cognizant DAA.

15. Access Warning. A warning against unauthorized access will be displayed (physically or electronically) on all visual display devices, cathode ray tubes (CRTs) or other input/output devices upon initial connection, log-on or system start-up of all computer systems (direct or remote access). AISs operating in the dedicated and system high security mode may use printed labels conspicuously applied to operator visible components stating the highest level of classified information allowed on that component.

16. Security Levels. When specified by SECNAV or OPNAV all SPAWAR AISs, networks or other computer resources developed or acquired must meet at least C2 level functionality as described in DoD 5200.28-STD. Hardware and software security requirements of computer resources should be determined in accordance with DoD 5200.28-STD.

17. Security Training and Awareness. There shall be in-place a Security Training and Awareness program to provide training for the security needs of all persons accessing an AIS, network or computer resource. The program shall ensure that all persons responsible for an AIS, network, computer resource and/or the information contained therein and all persons who must access them are aware of proper operational and security-related procedures and risks.

18. Operational Data. No classified or sensitive unclassified data shall be introduced into an SPAWAR AIS, network or computer resource without first identifying its classification or sensitivity.

19. Communications Security. All SPAWAR activities will establish measures designed to deny unauthorized persons information of value which might be derived from the possession, study or interpretation of telecommunications.

a. Communications Links. Transmission and communication lines and links which provide secure communication between components of a SPAWAR AIS authorized to process classified data will be secured in a manner appropriate to the highest classification of the material transmitted through such lines or links.

b. Interface with Communications Security. SPAWAR activities and HQ components that operate an AIS requiring only communication support from telecommunications networks will follow applicable Navy communications directives for the handling of classified material.

(1) The security measures will be agreed to and implemented before connecting to the communication network.

(2) They will be limited to those needed to ensure the development, interface and integration of secure, reliable, survivable and cost-effective transmission and communication lines and links to meet the communication requirements of the telecommunications network supporting system.

20. Color Coding. Color coding of magnetic media or components shall comply with OPNAVINST 5510.1H and the use of Standard Forms 706, 707, 709, 710, and 711 is mandatory.

21. Removable Media. The use of removable, securable, data storage systems is encouraged. The use of fixed internal hard disks to process classified and/or sensitive unclassified critical data are to be avoided. Authority to process classified data on this media must be approved by the cognizant DAA(s).

22. Emergency Destruction. The requirement to establish a policy for the destruction of media, networks and resources in the event of an emergency shall be addressed in the overall risk management and contingency planning programs.

23. Degaussing. Commands are encouraged to acquire and use NSA approved degaussing equipment.

24. Passwords. Systems which require the use of passwords shall comply with the requirements of CSC-STD-002-85.

SECTION 3

0909. DEFINITION OF TERMS

The following terms are used in the DON and SPAWAR AIS security programs:

1. Asset. Any software, data, hardware, administrative, physical, communications, or personnel resource within an automated information system or network.

2. Automated Information Systems (AIS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

3. Compromising Emanations. Unintentional relay of intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled or otherwise processed by any information processing equipment. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations.

4. Computer Resources. All resources related to computers and their management; including personnel, equipment, funds and technology.

5. Computer Security. Measures required to protect against unauthorized (accidental or intentional) disclosure, modification or destruction of AIS, networks and computer resources or denial of service to process data. It includes consideration of all hardware and software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS or network and for the data or information contained therein.

6. Contingency Plan. A plan for emergency response, backup operations, and post-disaster recovery, maintained by an activity as a part of its security program. A comprehensive statement of all the planned actions to be taken before, during and after a disaster or emergency condition including documented, tested procedures which will ensure the availability of critical computer resources and which will facilitate maintaining the continuity of operations in an emergency situation.

7. Countermeasure. Any action, device, procedure, technique or other measure that reduces the vulnerability of a system or activity to the realization of a threat.

8. Data Integrity. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, unauthorized disclosure or destruction.

9. Denial of Service. Action or actions that result in the ability of an AIS or any essential component to perform is designated mission, either by loss or degradation of operational capability.

10. Intelligence. Intelligence refers to foreign intelligence and counter intelligence involving sensitive sources or methods. Intelligence also includes SCI and all information that is (or should be) marked WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED (WNINTEL).

11. Need-To-Know. The necessity for access to knowledge of or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require possession of or access to such information and whether the individual is authorized to receive it rests with the individual having current possession, knowledge or control of the information involved and not with the prospective recipient.

12. Network. The interconnection of two or more independent computer facilities that provides for the transfer or sharing of computer system assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers and technical control devices.

13. Password. A protected word or sequence of characters that identifies or authenticates a user for access to a specific resource such as a data set, file or record.

14. Research, Development and Acquisition Process Acquired Mission-Critical Computer Resources (RDA-MCCR). Includes computer resources acquired under RDA procedures for use as integral parts of weapons; command and control; communications; intelligence; and other tactical or strategic systems aboard ships, aircraft and shore facilities and their support systems.

15. Risk. A measure of a system's exposure to harm.

16. Risk Assessment. An analysis of computer system and network assets, vulnerabilities and threats to determine the security requirements which must be satisfied to ensure that the system can be operated at an acceptable level of risk.

17. Risk Management. A methodology which provides an approach through which undersirable events can be identified, measured, controlled and prevented so as to effectively minimize their impact or frequency of occurrence. The fundamental element of risk management is the identification of the security posture, i.e., the characteristics of the functional environment from a security perspective. Risk management identifies the impact of events on the security posture and determines whether or not such impact is acceptable and, if not acceptable, provides for corrective action.

18. Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS, network or computer resource. Those safeguards may include but are not necessarily limited to: hardware and software security features, operational procedures, accountabilty procedures, access and distribution controls, management constraints, personnel security and physical structures, areas and devices.

19. Sensitive Compartmented Information (SCI). Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

20. Sensitive Unclassified Information. Any information the loss, misuse or unauthorized access to or modification of which could adversely affect the national interest, the conduct of DON and SPAWAR programs or the privacy of personnel (e.g., FOIA exempt information and information whose distribution is limited by OPNAVINST 5510.161).

21. SIOP-ESI. An acronym for Single Integrated Operational Plan - Extremely Sensitive Information; a DoD Special Access program.

22. Telecommunications. Any transmission, emission, or reception of signs, signals, writing, images, sounds, or information of any nature, by wire, radio, visual, or other electromagnetic systems.

EXHIBIT 12B

PROCEDURES FOR ASSIGNING DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS

PROCEDURES

1. Newly generated unclassified technical documents will be assigned Distribution Statement A, B, C, D, E, F, or X. Existing unclassified technical documents will be assigned Distribution Statement A, B, C, D, E, F or X if they have not already been made generally available to the public and if they are likely to be disseminated outside the Department of Defense. Technical documents in preliminary or working draft form will not be disseminated without a proper security classification review and assignment of a distribution statement.

2. Classified technical documents will be assigned Distribution Statement B, C, D, E or F. The distribution statement assigned to a classified document will be retained on the document after declassification or until the originating command specifically changes or removes it. If a technical document without a distribution statement is declassified, it will be handled the same as Distribution Statement F documents until changed by the originating command.

3. If a newly generated technical document contains export-controlled technical data, it will be marked with the statement in paragraph 1 under "ADDITIONAL NOTICES", in addition to Distribution Statement B, C, D, E, F or X.

4. Scientific and technical documents which include a contractor-imposed "limited rights" statement will be appropriately marked and controlled. (See "CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS" below.)

5. The distribution statement will be displayed conspicuously so it will be recognized readily by recipients. For standard written or printed material, the distribution statement will appear on the front cover, title page, and DD Form 1473, "Report Documentation Page". When possible, parts that contain information creating the requirement for the distribution statement will be prepared as an appendix to permit broader distribution of the basic document. When practicable, the abstract of the document, the DD Form 1473 and bibliographic citations will be written in such a way that the information will not be subject to Distribution Statement B, C, D, E, F or X. If the technical information is not in standard written or printed form and does not have a cover or title page, the distribution statement will be conspicuously stamped, printed, written or affixed by other means.

6. Distribution statements remain in effect until changed or removed by the originating command. Each command will establish and maintain a procedure for review of technical documents for which it is responsible, with the objective

of increasing their availability as soon as conditions permit. Public release determinations will be processed in accordance with references (cc) and (dd). When public release clearance is obtained, Distribution Statement A will be assigned and document handling facilities, including Defense Technical Information Center (DTIC), will be notified.

7. Technical documents with superseded distribution limitation markings will be reviewed and assigned the appropriate distribution statement when a request for the document is received. Superseded distribution limitation markings will be converted as follows:

a. Documents with distribution marking A or B need not be re-evaluated or remarked.

b. Documents with distribution marking #2 will be assigned Distribution Statement C.

c. Documents with distribution marking #3 (U.S. Government Only) will be assigned Distribution Statement B.

d. Documents with distribution marking #4 (DOD Only) will be assigned Distribution Statement E.

e. Documents with distribution marking #5 (Controlled) will be assigned Distribution Statement F.

8. Originating commands will promptly notify Defense Technical Information Center and other information repositories holding their technical documents when:

a. Address of designated originating commands is changed.

b. The originating command is redesignated.

c. Classification markings, distribution statements or export control statements are changed.

DISTRIBUTION STATEMENTS

The following distribution statements are authorized for use on technical documents:

1. **DISTRIBUTION STATEMENT A:** Approved for public release; distribution is unlimited.

a. This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority in accordance with references (cc) and (dd).

b. Technical documents resulting from contracted fundamental research efforts will normally be assigned Distribution Statement A, except for those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded in the contract or grant.

c. Technical documents with this statement may be made available or sold to the public including foreign nationals, companies, and governments, and may be exported.

d. This statement may never be used on technical documents that formerly were classified without a positive determination of such releasability by the command exercising cognizance over the information prior to release.

e. THIS STATEMENT WILL NOT BE USED ON CLASSIFIED TECHNICAL DOCUMENTS OR DOCUMENTS CONTAINING EXPORT-CONTROLLED TECHNICAL DATA AS PROVIDED IN OPNAVINST 5510.161 REFERENCE (jj).

2. **DISTRIBUTION STATEMENT B:** Distribution authorized to U.S. Government agencies only; (fill in reason) (date). Other requests for this document must be referred to (insert originating command).

a. This statement may be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement B include:

Foreign Government - To protect and limit information distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type is normally classified at the CONFIDENTIAL level or higher.

Proprietary Information - To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it may not be routinely transmitted outside the U.S. Government.

Critical Technology - To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of OPNAVINST 5510.161, reference (jj).

Test & Evaluation - To protect results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

Contractor Performance Evaluation - To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Premature Dissemination - To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.

Administrative/Operational Use - To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation - Releasable only in accordance with the provisions of SECNAVINST 5237.2 (NOTAL), reference (kk).

Specific Authority - To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DOD or DON regulations or policy guidance. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

3. **DISTRIBUTION STATEMENT C:** Distribution authorized to U.S. Government agencies and their contractors; (fill in reason) (date). Other requests for this document will be referred to (insert originating command).

a. May be used on unclassified technical documents, or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement C include:

(1) Foreign Government Information - Same as Distribution Statement B.

(2) Critical Technology - Same as Distribution Statement B.

(3) Software Documentation - Same as Distribution Statement B.

(4) Administrative or Operational Use - Same as Distribution Statement B.

(5) Specific Authority - Same as Distribution Statement B.

4. **DISTRIBUTION STATEMENT D:** Distribution authorized to DOD and DOD contractors only; (fill in reason) (date). Other U.S. requests shall be referred to (insert originating command).

a. May be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement D include:

(1) Foreign Government Information - Same as Distribution Statement B.

(2) Administrative or Operational Use - Same as Distribution Statement B.

(3) Software Documentation - Same as Distribution Statement B.

(4) Critical Technology - Same as Distribution Statement B.

(5) Specific Authority - Same as Distribution Statement B.

5. **DISTRIBUTION STATEMENT E:** Distribution authorized to DOD components only; (fill in reason) (date). Other requests must be referred to (insert originating command).

a. May be used on unclassified technical documents or on classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

b. Reasons for assigning Distribution Statement E include:

(1) Direct Military Support - Document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States. Designation of such data is made by competent authority in accordance with OPNAVINST 5510.161, reference (jj).

(2) Foreign Government Information - Same as Distribution Statement B.

(3) Proprietary Information - Same as Distribution Statement B.

(4) Premature Dissemination - Same as Distribution Statement B.

(5) Test and Evaluation - Same as Distribution Statement B.

(6) Software Documentation - Same as Distribution Statement B.

(7) Contractor Performance Evaluation - Same as Distribution Statement B.

(8) Critical Technology - Same as Distribution Statement B.

(9) Administrative/Operational Use - Same as Distribution Statement B.

(10) Specific Authority - Same as Distribution Statement B.

6. **DISTRIBUTION STATEMENT F:** Further dissemination only as directed by (insert originating command) (date) or higher DOD authority.

a. Normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists.

b. Distribution Statement F is used when the originator determines that the information is subject to the special dissemination limitation specified by paragraph 9-32.2a.

c. When a classified document assigned Distribution Statement F is declassified, the statement will be retained until the originating command assigns the proper distribution statement.

7. **DISTRIBUTION STATEMENT X:** Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with OPNAVINST 5510.161, reference (jj). Other requests must be referred to (originating command).

a. This statement will be used on unclassified documents when Distribution Statements B, C, D, E or F are not applicable but the document contains technical data as explained in OPNAVINST 5510.161, reference (jj).

b. This statement will not be used on classified technical documents. It may be assigned to technical documents that formerly were classified.

ADDITIONAL NOTICES

In addition to the distribution statement, the following notices will be used when appropriate:

1. All technical documents determined to contain export-controlled technical data will be marked "WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec. 2751 **et seq.**) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App 2401, **et seq.** Violations of these export laws are subject to

severe criminal penalties. Disseminate in accordance with provisions of OPNAVINST 5510.161, reference (jj)." When it is technically infeasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data" required by OPNAVINST 5510.161, reference (jj).

2. **Handling and Destroying Unclassified/Limited Distribution Documents.** Unclassified/Limited Distribution documents shall be handled using the same standard as "For Official Use Only (FOUO)" material, and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicate that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balanced against the degree of sensitivity.

CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS

1. Contractors may have proprietary technical data to which the Government is given limited rights. The contractor will place a limited rights statement on each document containing contractor-controlled technical data furnished to the Government. Documents with limited rights information will be assigned Distribution Statements B, E, or F.

2. Limited rights is defined as the right to use, duplicate, or disclose technical data in whole or in part, by or for the U.S. Government with the expressed limitation that, such technical data, without the written permission of the party furnishing the technical data, may not be:

a. Released or disclosed in whole or in part outside the Government.

b. Used in whole or in part by the Government for manufacture, or in the case of computer software documentation, for reproduction of the computer software.

c. Used by a party other than the Government, except for:

(1) Emergency repair or overhaul work only by or for the Government, when the item or process concerned is not otherwise reasonably available to enable timely performance of the work, provided that the release or disclosure outside the Government will be made subject to a prohibition against further use, release or disclosure, or

(2) Release to a foreign government, as the interest of the United States may require, only for information or evaluation within the foreign government or for emergency repair or overhaul work by or for the foreign government under the conditions of subparagraph (1).

3. The limited rights statement remains in effect until changed or cancelled under contract terms or with the permission of the contractor and the controlling office notifies recipients of the document that the statement has been changed or cancelled. Upon cancellation of the limited rights statement, the distribution, disclosure, or release of the technical document will then be controlled by its security classification or, if it is unclassified, by assignment of the appropriate Distribution Statement.